Cisco ASA シリーズ コマンド リファレンス、S コマンド

Cisco Systems, Inc.
http://www.cisco.com/jp

Cisco は世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は
当社の Web サイトをご覧ください。
www.cisco.com/go/offices をご覧ください。

Text Part Number: なし、オンライン専用

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco ASA シリーズ コマンド リファレンス、S コマンド

same-security-traffic through share-ratio コマンド

same-security-traffic

同じセキュリティレベルのインターフェイス間での通信を許可するか、またはトラフィックが同じインターフェイスに入って同じインターフェイスから出ることを許可するには、グローバル コンフィギュレーション モードで **same-security-traffic** コマンドを使用します。同じセキュリティレベルのトラフィックをディセーブルにするには、このコマンドの **no** 形式を使用します。

same-security-traffic permit {**inter-interface** | **intra-interface**}

no same-security-traffic permit {**inter-interface** | **intra-interface**}

構文の説明

inter-interface	同じセキュリティ レベルを持つ異なるインターフェイス間での通信を許可します。
intra-interface	同じインターフェイスに入って同じインターフェイスから出る通信を許可します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	**intra-interface** キーワードを使用すると、IPsec トラフィックだけではなく、すべてのトラフィックが同じインターフェイスに出入りできるようになりました。

使用上のガイドライン

同じセキュリティ レベルのインターフェイス間での通信を許可すると（**same-security-traffic inter-interface** コマンドを使用してイネーブルにします）、次の利点があります。

- 101 より多い数の通信インターフェイスを設定できます。各インターフェイスで異なるレベルを使用する場合は、レベルごと（0 ～ 100）に 1 つのインターフェイスのみを設定できます。
- アクセス リストなしで、すべての同じセキュリティ レベルのインターフェイス間で自由にトラフィックを送受信できます。

same-security-traffic intra-interface コマンドを使用すると、トラフィックが同じインターフェイスに入って同じインターフェイスから出ることができます。この動作は、通常は許可されていません。この機能は、あるインターフェイスに入り、その後同じインターフェイスからルーティングされる VPN トラフィックの場合に役立ちます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブ アンド スポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注） **same-security-traffic intra-interface** コマンドによって許可されるすべてのトラフィックには、引き続きファイアウォール ルールが適用されます。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

例

次に、同じセキュリティ レベルのインターフェイス間での通信をイネーブルにする例を示します。

```
ciscoasa(config)# same-security-traffic permit inter-interface
```

次に、トラフィックが同じインターフェイスに入って同じインターフェイスから出られるようにする例を示します。

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

関連コマンド

コマンド	説明
show running-config same-security-traffic	**same-security-traffic** コンフィギュレーションを表示します。

sasl-mechanism

LDAP クライアントを LDAP サーバに対して認証するための Simple Authentication and Security Layer（SASL）メカニズムを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **sasl-mechanism** コマンドを使用します。SASL 認証メカニズムのオプションは、**digest-md5** および **kerberos** です。

認証メカニズムをディセーブルにするには、このコマンドの **no** 形式を使用します。

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

(注) VPN ユーザにとっては、ASA が LDAP サーバへのクライアント プロキシとして動作するため、ここでの LDAP クライアントとは ASA を意味しています。

構文の説明

digest-md5	ASA は、ユーザ名とパスワードから計算された MD5 値を使用して応答します。
kerberos	ASA は、Generic Security Services Application Programming Interface（GSSAPI）Kerberos メカニズムを使用してユーザ名とレルムを送信することによって応答します。
server-group-name	最大 64 文字の Kerberos AAA サーバ グループを指定します。

デフォルト

デフォルトの動作や値はありません。ASA は、認証パラメータをプレーン テキストで LDAP サーバに渡します。

(注) SASL を設定していない場合は、**ldap-over-ssl** コマンドを使用して、SSL によって LDAP 通信を保護することを推奨します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA が SASL メカニズムを使用して LDAP サーバに対する認証を行うよう指定するには、このコマンドを使用します。

ASA と LDAP サーバの両方で、複数の SASL 認証メカニズムをサポートできます。SASL 認証をネゴシエートする場合、ASA はサーバに設定されている SASL メカニズムのリストを取得して、ASA とサーバの両方に設定されているメカニズムのうち最も強力な認証メカニズムを設定します。Kerberos メカニズムは、Digest-MD5 メカニズムよりも強力です。たとえば、LDAP サーバと ASA の両方でこれら 2 つのメカニズムがサポートされている場合、ASA では、より強力な Kerberos メカニズムが選択されます。

各メカニズムは独立して設定されるため、SASL メカニズムをディセーブルにするには、ディセーブルにする各メカニズムに対して別々に **no** コマンドを入力する必要があります。明示的にディセーブルにしないメカニズムは引き続き有効です。たとえば、両方の SASL メカニズムをディセーブルにするには、次の両方のコマンドを入力する必要があります。

no sasl-mechanism digest-md5

no sasl-mechanism kerberos *server-group-name*

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、名前が ldapsvr1、IP アドレスが 10.10.0.1 の LDAP サーバに対する認証のために SASL メカニズムをイネーブルにする例を示します。この例では、SASL digest-md5 認証メカニズムがイネーブルにされています。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism digest-md5
```

次に、SASL Kerberos 認証メカニズムをイネーブルにして、Kerberos AAA サーバとして kerb-servr1 を指定する例を示します。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL が LDAP クライアントとサーバ間の接続を保護することを指定します。
server-type	LDAP サーバ ベンダーに Microsoft または Sun のいずれかを指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

saml idp

新しい SAML IdP を追加するには、webvpn コンフィギュレーション モードで **saml idp** コマンドを使用します。SAML IdP を削除するには、このコマンドの **no** 形式を使用します。

saml idp *idp-entityID*

no saml idp *idp-entityID*

構文の説明

base-URL	クライアントレス VPN のベース URL。サードパーティ製 IdP に提供される SAML メタデータで使用されます。それによって、IdP はエンドユーザを ASA へリダイレクトできます。
idp-entityID	ASA が使用するように設定している SAML Idp のエンティティ ID。
internal	IdP が内部ネットワーク内にある場合は、このフラグを設定します。
シグニチャ **signature <value>**	SAML 要求内の署名を有効または無効にします。 （オプション）署名を有効にし、SAML 要求で特定の方式を使用します。
timeout assertion	NotBefore とタイムアウトの合計が NoOnOrAfter より早い場合に、NoOnOrAfter を上書きします。
timeout-in-seconds	SAML タイムアウト値（秒単位）。デフォルトでは、SAML タイムアウトは設定されていません。アサーションの NotBefore と NotOnOrAfter は、有効性を判別するために使用されます。
trustpoint [idp | sp] ***<trustpoint-name>***	トラストポイント idp には、SAML アサーションを検証するための ASA の IdP 証明書が含まれます。 trustpoint-name は、既存のトラストポイント名のいずれかになります。 トラストポイント sp には、ASA の署名を検証するか、または SAML アサーションを暗号化するための IdP の ASA（SP）証明書が含まれます。
url [sign-in | sign-out] ***<value>***	URL は、IdP のサインインおよびサインアウト URL です。 IdP にサインインするための URL の値。url 値には、4 ～ 2000 文字を含める必要があります。

デフォルト

なし。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。
9.7(1)	internal 属性が追加されました。
9.8(1)	SHA2 サポートと署名方式を指定する機能が SAML 要求に追加されました。

使用上のガイドライン

このコマンドは、1 つ以上のサードパーティの SAML ID プロバイダーの設定値を設定します。IdP 設定は、それらがトンネル グループに適用されるまで使用されません。

SAML IdP のサインイン URL、サインアウト URL、署名証明書は、ベンダーの Web サイトで確認できます。IdP の署名証明書を保持するためのトラストポイントを作成する必要があります。トラストポイント名はトラストポイント idp によって使用されます。

webvpn モードで Idp を作成すると、saml-idp サブモードに切り替わります。このモードで、この Idp の次の設定値を設定できます。

- url sign-in：Idp にサインインするための URL。
- url sign-out：IdP をサインアウトしたときのリダイレクト先 URL。
- signature：SAML 要求内の署名を有効または無効にします。デフォルトでは、署名は無効になっています。
- signature <value>：署名を有効にし、rsa-sha1、rsa-sha256、rsa-sha384、または rsa-sha512 を方式に指定します。デフォルトでは、署名は無効になっています。
- time-out：SAML タイムアウト値（秒単位）。
- base-url：エンドユーザを ASA にリダイレクトするために、URL がサードパーティ IdP に提供されます。base-url を設定しないと、URL は ASA のホスト名とドメイン名から取得されます。たとえば、ホスト名が「ssl-vpn」で、ドメイン名が「cisco.com」の場合、show saml metadata では、https://ssl-vpn.cisco.com がベース URL として表示されます。base-url またはホスト名/ドメイン名のいずれも設定されていない場合、show saml metadata はエラーを返します。
- trustpoint：ASA の署名を検証するか、または SAML アサーションを暗号化するために、ASA（SP）に基づく既存のトラストポイントまたは IdP が使用できる IDP 証明書を割り当てます。

例

次に、Idp を定義し、Idp 設定値を設定する方法の例を示します。

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config-webvpn)# saml idp salesforce_idp
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)# trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_trustpoint
ciscoasa(config-webvpn)# saml idp feide_idp
ciscoasa(config-webvpn-saml-idp)# url sign-in
http://cisco.feide.no/simplesaml/saml2/idp/SSOService.php
ciscoasa(config-webvpn-saml-idp)# trustpoint idp feide_trustpoint
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_trustpoint
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 120
ciscoasa(config-webvpn-saml-idp)# base-url https://ssl-vpn.cisco.com
```

関連コマンド

コマンド	説明
authentication	saml などの、トンネル グループの認証タイプを設定します。
identity-provider	ASA 内のサードパーティ SAML ID プロバイダーのこの設定に名前を付けます。

saml identity-provider

config-tunnel-webvpn モードでこの CLI を使用して、SAML IdP をトンネル グループ（接続プロファイル）に割り当てます。

saml identity-provider *name*

no saml identity-provider *name*

構文の説明

name	ASA が使用するように設定している SAML Idp の名前。

デフォルト

なし。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

これは、ASA 内のサードパーティ SAML ID プロバイダーのこの設定に名前を付けます。

関連コマンド

コマンド	説明
authentication	saml などの、トンネル グループの認証タイプを設定します。
idp	サードパーティ SAML ID プロバイダーの Idp を設定します。

sast

CTL レコードに作成する SAST 証明書の数を指定するには、CTL ファイル コンフィギュレーション モードで **sast** コマンドを使用します。CTL ファイル内の SAST 証明書の数をデフォルト値の 2 に戻すには、このコマンドの **no** 形式を使用します。

sast *number_sasts*

no sast *number_sasts*

構文の説明

number_sasts	作成する SAST キーの数を指定します。デフォルトは 2 です。許容最大数は、5 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ctl ファイル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。

使用上のガイドライン

CTL ファイルは、System Administrator Security Token（SAST; システム管理者セキュリティ トークン）によって署名されます。

電話プロキシは CTL ファイルを生成するため、CTL ファイル自体を署名するための SAST キーを作成する必要があります。このキーは、ASA で生成できます。SAST は、自己署名証明書として作成されます。

通常、CTL ファイルには複数の SAST が含まれています。ある SAST が回復可能でない場合は、後でもう 1 つの SAST を使用してファイルを署名できます。

例

次に、**sast** コマンドを使用して、CTL ファイルに 5 つの SAST 証明書を作成する例を示します。

```
ciscoasa(config-ctl-file)# sast 5
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file（Phone-Proxy）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

scansafe

コンテキストに対してクラウド Web セキュリティ インスペクションをイネーブルにするには、コンテキスト コンフィギュレーション モードで **scansafe** コマンドを使用します。クラウド Web セキュリティをディセーブルにするには、このコマンドの **no** 形式を使用します。

scansafe [**license** *key*]

no scansafe [**license** *key*]

構文の説明

license *key*	このコンテキストの認証キーを入力します。キーを指定しない場合は、システム コンフィギュレーションで設定されているライセンスがこのコンテキストで使用されます。ASA は、要求がどの組織からのものかを示すために、認証キーを クラウド Web セキュリティ プロキシ サーバに送信します。認証キーは 16 バイトの 16 進数です。

コマンド デフォルト

デフォルトでは、システム コンフィギュレーションに入力されたライセンスがコンテキストで使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可する必要があります。

例

次に、デフォルトのライセンスを使用してコンテキスト 1 でクラウド Web セキュリティをイネーブルにし、ライセンス キーの上書きを使用してコンテキスト 2 でクラウド Web セキュリティをイネーブルにする設定の例を示します。

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
```

```
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

scansafe general-options

クラウド Web セキュリティ プロキシ サーバとの通信を設定するには、グローバル コンフィギュレーション モードで **scansafe general-options** コマンドを使用します。サーバ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

scansafe general-options

no scansafe general-options

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

クラウド Web セキュリティのプライマリ プロキシ サーバとバックアップ プロキシ サーバを設定できます。

例

次に、プライマリ サーバを設定する例を示します。

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
health-check application	フェールオーバーのための、クラウド Web セキュリティのアプリケーション健全性チェックを有効にします。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

scep-enrollment enable

トンネル グループの Simple Certificate Enrollment Protocol をイネーブルまたはディセーブルにするには、トンネル グループ一般属性モードで **scep-enrollment enable** コマンドを使用します。

このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

scep-enrollment enable

no scep-enrollment enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、このコマンドはトンネル グループ コンフィギュレーションに存在しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

この機能がサポートされるのは、リリース 3.0 以降の Cisco AnyConnect Secure Mobility Client のみです。

ASA は、AnyConnect とサードパーティ認証局の間の SCEP 要求のプロキシとして動作することができます。認証局がプロキシとして動作する場合に必要なのは、ASA にアクセス可能であることのみです。ASA のこのサービスが機能するには、ASA が登録要求を送信する前に、ユーザが AAA でサポートされているいずれかの方法を使用して認証されている必要があります。また、ホスト スキャンおよびダイナミック アクセス ポリシーを使用して、登録資格のルールを適用することもできます。

ASA では、AnyConnect SSL または IKEv2 VPN セッションでのみこの機能をサポートしています。これは、IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含む、すべての SCEP 準拠認証局をサポートしています。

クライアントレス（ブラウザベース）でのアクセスは SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）はサポートしていません。

ASA では、証明書のポーリングはサポートしていません。

ASA はこの機能に対するロード バランシングをサポートしています。

例

次に、グローバル コンフィギュレーション モードで、remotegrp というリモート アクセス トンネル グループを作成し、グループ ポリシー用の SCEP をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this
option.
```

関連コマンド

コマンド	説明
crypto ikev2 enable	IPsec ピアが通信するインターフェイスで IKEv2 ネゴシエーションをイネーブルにします。
scep-forwarding-url	グループ ポリシー用の SCEP 認証局を登録します。
secondary-pre-fill-username clientless	証明書が SCEP プロキシの WebLaunch のサポートに使用できない場合は、共通のセカンダリ パスワードを使用します。
secondary-authentication-server-group	証明書が使用できないときにはユーザ名を指定します。

scep-forwarding-url

グループ ポリシー用の SCEP 認証局を登録するには、グループ ポリシー コンフィギュレーション モードで **scep-forwarding-url** コマンドを使用します。

このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

scep-forwarding-url {**none** | **value** [*URL*]}

no scep-forwarding-url

構文の説明

none	グループ ポリシーの認証局を指定しません。
URL	認証局の SCEP URL を指定します。
value	この機能をクライアントレス接続でイネーブルにします。

デフォルト

デフォルトでは、このコマンドは存在しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、サードパーティのデジタル証明書をサポートするグループ ポリシーごとに 1 回入力します。

Example

次に、グローバル コンフィギュレーション モードで、FirstGroup という名前のグループ ポリシーを作成し、グループ ポリシーの認証局を登録する例を示します。

```
ciscoasa(config)# group-policy FirstGroup internal
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
Attempting to retrieve the CA/RA certificate(s) using the URL. Please wait ...
```

関連コマンド

コマンド	説明
crypto ikev2 enable	IPsec ピアが通信するインターフェイスで IKEv2 ネゴシエーションをイネーブルにします。
scep-enrollment enable	トンネル グループに対して Simple Certificate Enrollment Protocol をイネーブルにします。
secondary-pre-fill-username clientless	証明書が SCEP プロキシの WebLaunch のサポートに使用できない場合は、共通のセカンダリ パスワードを使用します。
secondary-authentication-server-group	証明書が使用できないときにはユーザ名を指定します。

secondary

preempt コマンドの使用時にフェールオーバー グループの優先ユニットを設定するには、フェールオーバー グループ コンフィギュレーション モードで **secondary** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

secondary

no secondary

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

フェールオーバー グループに **primary** または **secondary** が指定されていない場合は、フェールオーバー グループはデフォルトで **primary** に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	早期のソフトウェア バージョンでは、フェールオーバー グループが優先ユニットでアクティブになるために **preempt** コマンドを必要としないように、「同時」ブートアップが許可されていました。ただし、この機能は、現在、両方のフェールオーバー グループがブートアップした最初のユニットでアクティブになるように変更されています。

使用上のガイドライン

primary または **secondary** 優先順位をフェールオーバー グループに割り当てると、**preempt** コマンドが設定されているときに、フェールオーバー グループがどのユニット上でアクティブになるかが指定されます。グループの **primary** または **secondary** の設定にかかわらず、両方のフェールオーバー グループがブートアップした最初のユニットでアクティブになります(それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります)。もう一方のユニットがオンラインになったとき、2 番めのユニットをプライオリティの高いユニットとして所有するフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。フェールオーバー グループが **preempt** コマンドで設定される場合、指定されたユニットでフェールオーバー グループが自動的にアクティブになります。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どのフェールオーバー グループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先するユニットが使用可能になったときにそのユニット上で自動的にアクティブになります。

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
preempt	優先するユニットが使用可能になったときに、フェールオーバー グループをそのユニット上で強制的にアクティブにします。
primary	プライマリ ユニットに、セカンダリ ユニットよりも高いプライオリティを付与します。

secondary-authentication-server-group

二重認証がイネーブルの場合にセッションに関連付けるセカンダリ認証サーバ グループを指定するには、トンネル グループ一般属性モードで **secondary-authentication-server-group** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

secondary-authentication-server-group [*interface_name*] {**none** | **LOCAL** | *groupname* [**LOCAL**]} [**use-primary-username**]}

no secondary-authentication-server-group

構文の説明

interface_name	(オプション)IPsec トンネルが終端するインターフェイスを指定します。
LOCAL	(任意)通信障害によりサーバ グループにあるすべてのサーバが非アクティブになった場合に、ローカル ユーザ データベースに対する認証を要求します。サーバ グループ名が **LOCAL** または **NONE** の場合、ここでは **LOCAL** キーワードを使用しないでください。
none	(任意)サーバ グループ名を **NONE** と指定して、認証が不要であることを示します。
groupname [**LOCAL**]	事前に設定済みの認証サーバまたはサーバ グループを指定します。LOCAL グループを指定することもできます。
use-primary-username	プライマリ ユーザ名をセカンダリ認証のユーザ名として使用します。

デフォルト

デフォルト値は **none** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。**secondary-authentication-server-group** コマンドは、セカンダリ AAA サーバ グループを指定します。SDI サーバ グループはセカンダリ サーバ グループにできません。

use-primary-username キーワードが設定されている場合は、ログイン ダイアログボックスで 1 つのユーザ名のみが要求されます。

ユーザ名がデジタル証明書から抽出される場合は、プライマリ ユーザ名だけが認証に使用されます。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループを作成して、接続のプライマリ サーバ グループとしてグループ sdi_server の使用を指定し、セカンダリ認証サーバ グループとしてグループ ldap_server を指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-server-group sdi_server
ciscoasa(config-tunnel-webvpn)# secondary-authentication-server-group ldap_server
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザ名機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。
username-from-certificate	認可時のユーザ名として使用する証明書内のフィールドを指定します。

secondary-color

WebVPN ログイン、ホームページ、およびファイル アクセス ページのセカンダリ カラーを設定するには、webvpn コンフィギュレーション モードで **secondary-color** コマンドを使用します。色をコンフィギュレーションから削除して、デフォルトにリセットするには、このコマンドの **no** 形式を使用します。

secondary-color [*color*]

no secondary-color

構文の説明

color	(任意)色を指定します。カンマ区切りの RGB 値、HTML の色値、または色の名前(HTML で認識される場合)を使用できます。 • RGB 形式は 0,0,0 で、各色(赤、緑、青)を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。 • HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。 • 名前の最大長は 32 文字です。

デフォルト

デフォルトのセカンダリ カラーは HTML の #CCCCFF(薄紫色)です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

RGB 値を使用する場合、推奨値は 216 です。推奨色は、数学的にあり得る数よりはるかに少なくなります。多くのディスプレイは 256 色しか処理できず、そのうちの 40 色は MAC と PC とでは異なった表示になります。最適な結果を得るために、公開されている RGB テーブルをチェックしてください。RGB テーブルをオンラインで検索するには、検索エンジンで RGB と入力します。

例

次に、HTML の色値 #5F9EAO（灰青色）を設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# secondary-color #5F9EAO
```

関連コマンド

コマンド	説明
title-color	ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトル バーの色を設定します。

secondary-pre-fill-username

クライアントレスまたは AnyConnect 接続の二重認証で使用するクライアント証明書からユーザ名を抽出できるようにするには、トンネル グループ webvpn 属性モードで **secondary-pre-fill-username** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

secondary-pre-fill-username {**clientless** | **ssl-client**} [**hide**]

secondary-pre-fill-username {**clientless** | **ssl-client**} **hide** [**use-primary-password** | **use-common-password** [*type_num*] *password*]

no secondary-no pre-fill-username

構文の説明

clientless	この機能をクライアントレス接続でイネーブルにします。
hide	認証に使用するユーザ名を VPN ユーザに非表示にします。
password	パスワード ストリングを入力します。
ssl-client	この機能を AnyConnect VPN クライアント接続でイネーブルにします。
type_num	次のいずれかのオプションを入力します。 • 入力するパスワードがプレーン テキストの場合は 0。 • 入力するパスワードが暗号化されている場合は 8。パスワードは、入力時にアスタリスクで表示されます。
use-common-password	ユーザにプロンプトを表示せずに、使用する共通の 2 次認証パスワードを指定します。
use-primary-password	ユーザにプロンプトを表示せずに、2 次認証に 1 次認証パスワードを再使用します。

デフォルト

この機能はデフォルトで無効に設定されています。**hide** キーワードを指定せずにこのコマンドを入力すると、抽出したユーザ名が VPN ユーザに表示されます。**use-primary-password** と **use-common-password** のいずれのキーワードも指定しないと、ユーザにはパスワード プロンプトが表示されます。*type_num* のデフォルト値は 8 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ webvpn 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.3(2)	[**use-primary-password** | **use-common-password** [*type_num*] *password*] オプションが追加されました。

使用上のガイドライン

この機能をイネーブルにするには、トンネル グループ一般属性モードで **secondary-username-from-certificate** コマンドを入力する必要もあります。

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。**secondary-pre-fill-username** コマンドは、**secondary-username-from-certificate** コマンドで指定された証明書フィールドから抽出されたユーザ名を、セカンダリ ユーザ名またはパスワード認証のユーザ名として使用できるようにします。2 回めの認証で証明書からのユーザ名の事前充填機能を使用するには、両方のコマンドを設定する必要があります。

(注) クライアントレス接続と SSL クライアント接続は、相互排他的なオプションではありません。1 つのコマンドラインで指定できるのはいずれか 1 つのみですが、同時に両方をイネーブルにできます。

2 番めの名を非表示にして、プライマリまたは共通のパスワードを使用する場合は、ユーザ体験は単一認証と似ています。プライマリまたは共通のパスワードを使用すると、デバイス証明書を使用したデバイスの認証がシームレスなユーザ体験になります。

use-primary-password キーワードは、すべての認証のセカンダリ パスワードとしてプライマリ パスワードを使用することを指定します。

use-common-password キーワードは、すべての 2 次認証に共通のセカンダリ パスワードを使用することを指定します。エンドポイントにインストールされているデバイス証明書に BIOS ID またはその他の ID が含まれている場合は、2 次認証要求では、事前に入力された BIOS ID をセカンダリ ユーザ名として使用して、そのトンネル グループでのすべての認証に対して設定された共通のパスワードを使用できます。

例

次の例では、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成して、接続がブラウザベースである場合に、エンドポイントのデジタル証明書の名前を、認証または認可クエリーに使用する名前として再使用することを指定します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless
```

次の例では、前のコマンドと同じ機能を実行しますが、抽出されたユーザ名をユーザに非表示にします。

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
```

次の例では、AnyConnect 接続だけに適用される点を除いて、前のコマンドと同じ機能を実行します。

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
```

次の例では、ユーザ名を非表示にして、ユーザにプロンプトを表示せずに、2 次認証に 1 次認証パスワードを再使用します。

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-primary-password
```

次の例では、ユーザ名を非表示にして、入力するパスワードを 2 次認証に使用します。

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password **********
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザ名機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。
username-from-certificate	認可時のユーザ名として使用する証明書内のフィールドを指定します。

secondary-text-color

WebVPN ログイン、ホームページ、およびファイル アクセス ページのセカンダリ テキストの色を設定するには、webvpn モードで **secondary-text-color** コマンドを使用します。色をコンフィギュレーションから削除して、デフォルトにリセットするには、このコマンドの **no** 形式を使用します。

secondary-text-color [*black* | *white*]

no secondary-text-color

構文の説明

auto	text-color コマンドの設定に基づいて、黒または白が選択されます。つまり、プライマリ カラーが黒の場合、この値は白になります。
black	デフォルトのセカンダリ テキストの色は黒です。
white	テキストの色を白に変更できます。

デフォルト

デフォルトのセカンダリ テキストの色は黒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、セカンダリ テキストの色を白に設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# secondary-text-color white
```

関連コマンド

コマンド	説明
text-color	ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトル バーのテキストの色を設定します。

secondary-username-from-certificate

クライアントレス接続または AnyConnect（SSL クライアント）接続において、二重認証の 2 つめのユーザ名として使用する証明書のフィールドを指定するには、トンネル グループ一般属性モードで **secondary-username-from-certificate** コマンドを使用します。

属性をコンフィギュレーションから削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

secondary-username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**}

no secondary-username-from-certificate

構文の説明

primary-attr	証明書から認可クエリーのユーザ名を取得するために使用する属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
secondary-attr	（任意）デジタル証明書から認証または認可クエリーのユーザ名を取得するためにプライマリ属性とともに使用する追加の属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
use-entire-name	ASA では、完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得する必要があることを指定します。
use-script	ASDM によって生成されたスクリプト ファイルを使用して、ユーザ名として使用する DN フィールドを証明書から抽出することを指定します。

デフォルト

この機能はデフォルトでディセーブルであり、二重認証がイネーブルの場合にのみ有効です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。

二重認証が有効になっている場合、このコマンドはユーザ名として使用する 1 つ以上のフィールドを証明書から選択します。**secondary-username-from-certificate** コマンドは、セキュリティアプライアンスに、指定した証明書フィールドを 2 回めのユーザ名/パスワード認証のための 2 つめのユーザ名として使用するように強制します。

2 回めのユーザ名/パスワード認証または認可のために、証明書からのユーザ名の事前充填機能で、取得されたユーザ名を使用するには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドおよび **secondary-pre-fill-username** コマンドも設定する必要があります。つまり、2 回めのユーザ名の事前充填機能を使用するには、両方のコマンドを設定する必要があります。

プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。
use-entire-name	DN 名全体を使用します。セカンダリ属性としては使用できません。
use-script	ASDM によって生成されたスクリプト ファイルを使用します。

（注） **secondary-authentication-server-group** コマンドを **secondary-username-from-certificate** コマンドとともに指定した場合は、プライマリ ユーザ名のみが認証に使用されます。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループを作成し、プライマリ属性として CN（一般名）、セカンダリ属性として OU を使用して、デジタル証明書から認可クエリーの名前を取得するように指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN
ciscoasa(config-tunnel-general)# secondary-username-from-certificate OU
ciscoasa(config-tunnel-general)#
```

次に、トンネル グループ属性を変更し、事前入力ユーザ名を設定する例を示します。

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザ名機能をイネーブルにします。
secondary-pre-fill-username	クライアントレス接続または AnyConnect クライアント接続において、ユーザ名抽出をイネーブルにします。
username-from-certificate	認可時のユーザ名として使用する証明書内のフィールドを指定します。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
secondary-authentication-server-group	セカンダリ AAA サーバ グループを指定します。ユーザ名がデジタル証明書から抽出される場合は、プライマリ ユーザ名だけが認証に使用されます。

secondary-username-from-certificate-choice

セカンダリ認証または許可用として事前入力ユーザ名フィールドにユーザ名を使用する必要がある証明書を選択するには、**secondary-username-from-certificate-choice** コマンドを使用します。このコマンドは tunnel-group general-attributes モードで使用します。デフォルトの証明書で使用されているユーザ名を使用するには、このコマンドの **no** 形式を使用します。

secondary-username-from-certificate-choice {**first-certificate** | **second-certificate**}

no secondary-username-from-certificate-choice {**first-certificate** | **second-certificate**}

構文の説明

first-certificate	マシン証明書のユーザ名を、セカンダリ認証の事前入力ユーザ名フィールドで使用するように SSL または IKE で送信するかどうかを指定します。
second-certificate	ユーザ証明書のユーザ名を、セカンダリ認証の事前入力ユーザ名フィールドで使用するようにクライアントから送信するかどうかを指定します。

デフォルト

デフォルトでは、事前入力するユーザ名は 2 つ目の証明書から取得されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

複数証明書オプションを使用すると、証明書を通じたマシンとユーザ両方の証明書認証が可能になります。事前入力ユーザ名フィールドでは、証明書のフィールドを解析し、AAA および証明書認証済み接続で以降の（プライマリまたはセカンダリ）AAA 認証に使用することができます。事前入力のユーザ名は、常にクライアントから受信した 2 つ目の（ユーザ）証明書から取得されます。

9.14(1) 以降、ASA では、最初の証明書（マシン証明書）または 2 つ目の証明書（ユーザ証明書）のどちらを使用して事前入力ユーザ名フィールドに使用するユーザ名を取得するかを選択できます。

このコマンドは、認証タイプ（AAA、証明書、または複数証明書）に関係なく、任意のトンネルグループに使用および設定できます。ただし、設定は、複数証明書認証（複数証明書または AAA 複数証明書）に対してのみ有効となります。このオプションが複数証明書認証に使用されない場合は、2 つ目の証明書がデフォルトとして認証または許可の目的で使用されます。

例

次に、プライマリおよびセカンダリ認証または許可の事前入力ユーザ名に使用する証明書を設定する方法の例を示します。

```
ciscoasa(config)#tunnel-group tg1 type remote-access
ciscoasa(config)#tunnel-group tg1 general-attributes
ciscoasa(config-tunnel-general)# address-pool IPv4
ciscoasa(config-tunnel-general)# secondary-authentication-server-group LOCAL/<Auth-Server>
ciscoasa(config-tunnel-general)# username-from-certificate-choice first-certificate
ciscoasa(config-tunnel-general)# secondary-username-from-certificate-choice
first-certificate

ciscoasa(config)# tunnel-group tg1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication aaa multiple-certificate
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client
```

関連コマンド

コマンド	説明
username-from-certificate-choice	プライマリ認証の証明書オプションを指定します。

secure-unit-authentication

セキュア ユニット認証をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **secure-unit-authentication enable** コマンドを使用します。セキュア ユニット認証をディセーブルにするには、**secure-unit-authentication disable** コマンドを使用します。実行コンフィギュレーションからセキュア ユニット認証属性を削除するには、このコマンドの **no** 形式を使用します。**secure-unit-authentication** {**enable** | **disable**}

no secure-unit-authentication

構文の説明

disable	セキュア ユニット認証をディセーブルにします。
enable	セキュア ユニット認証をイネーブルにします。

デフォルト

セキュア ユニット認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

セキュア ユニット認証では、ハードウェア クライアントが使用するトンネル グループに認証サーバ グループが設定されている必要があります。

プライマリASA でセキュア ユニット認証が必要な場合は、すべてのバックアップ サーバに対してもセキュア ユニット認証を設定する必要があります。

no オプションを指定すると、他のグループ ポリシーからセキュア ユニット認証の値を継承できます。

セキュア ユニット認証では、VPN ハードウェア クライアントがトンネルを開始するたびにクライアントに対してユーザ名/パスワード認証を要求することによって、セキュリティが強化されます。この機能をイネーブルにすると、ハードウェア クライアントではユーザ名とパスワードが保存されません。

（注） この機能をイネーブルにした場合に VPN トンネルを確立するには、ユーザがユーザ名とパスワードを入力する必要があります。

例

次に、FirstGroup という名前のグループ ポリシーに対して、セキュア ユニット認証をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# secure-unit-authentication enable
```

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を行わずに IP 電話に接続できるようにします。セキュア ユニット認証は有効なままです。
leap-bypass	イネーブルの場合、VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットがユーザ認証の前に VPN トンネルを通過できます。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。その後、ユーザ認証ごとに再度認証を行います。
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前に ASA に識別情報を示すように要求します。

security-group

Cisco TrustSec で使用できるようにセキュリティ グループをセキュリティ オブジェクト グループに追加するには、オブジェクトグループ セキュリティ コンフィギュレーション モードで **security-group** コマンドを使用します。セキュリティ グループを削除するには、このコマンドの **no** 形式を使用します。

security-group {**tag** *sgt#* | **name** *sg_name*}

no security-group {**tag** *sgt#* | **name** *sg_name*}

構文の説明

tag *sgt#*	セキュリティ グループ オブジェクトをインライン タグとして指定します。セキュリティ タイプがタグの場合は、1 ～ 65533 の数字を入力します。 SGT は、ISE による IEEE 802.1X 認証、Web 認証、または MAC 認証バイパス（MAB）を通してデバイスに割り当てられます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。
name *sg_name*	セキュリティ グループ オブジェクトを名前付きオブジェクトとして指定します。セキュリティ タイプが名前の場合は、32 バイトの文字列を、大文字と小文字を区別して入力します。*sg_name* には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] を含めることができます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
オブジェクトグループ セキュリティ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

作成したセキュリティ グループ オブジェクト グループは、Cisco TrustSec をサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールで使用できるようになります。

Cisco TrustSec と統合されているときは、ASA は ISE からセキュリティ グループの情報をダウンロードします。ISE はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザ アイデンティティへのマッピングと、Cisco TrustSec タグからサーバ リソースへのマッピングを行います。セキュリティ グループ アクセス リストのプロビジョニングおよび管理は、中央集中型で ISE 上で行います。

ただし、ASA には、グローバルには定義されていない、ローカライズされたネットワーク リソースが存在することがあり、そのようなリソースにはローカル セキュリティ グループとローカライズされたセキュリティ ポリシーが必要です。ローカル セキュリティ グループには、ISE からダウンロードされた、ネストされたセキュリティ グループを含めることができます。ASA は、ローカルと中央のセキュリティ グループを統合します。

ASA 上でローカル セキュリティ グループを作成するには、ローカル セキュリティ オブジェクト グループを作成します。1 つのローカル セキュリティ オブジェクト グループに、1 つ以上のネストされたセキュリティ オブジェクト グループまたはセキュリティ ID またはセキュリティ グループ名を入れることができます。ユーザは、ASA 上に存在しない新しいセキュリティ ID またはセキュリティ グループ名を作成することもできます。

ASA 上で作成したセキュリティ オブジェクト グループは、ネットワーク リソースへのアクセスの制御に使用できます。セキュリティ オブジェクト グループを、アクセス グループやサービス ポリシーの一部として使用できます。

例

次に、セキュリティ グループ オブジェクトを設定する例を示します。

```
ciscoasa(config)# object-group security mktg-sg
ciscoasa(config)# security-group name mktg
ciscoasa(config)# security-group tag 1
```

次に、セキュリティ グループ オブジェクトを設定する例を示します。

```
ciscoasa(config)# object-group security mktg-sg-all
ciscoasa(config)# security-group name mktg-managers
ciscoasa(config)# group-object mktg-sg // nested object-group
```

関連コマンド

コマンド	説明
object-group security	セキュリティ グループ オブジェクトを作成します。

security-group-tag

リモート アクセス VPN グループ ポリシーまたは LOCAL ユーザ データベース内のユーザのセキュリティ グループ タグを設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **security-group-tag value** コマンドを使用します。セキュリティ グループ タグ属性を削除するには、このコマンドの **no** 形式を使用します。

security-group-tag {**none** | **value** *sgt*}

no security-group-tag {**none** | **value** *sgt*}

構文の説明

none	このグループ ポリシーまたはユーザのセキュリティ グループ タグを設定しません。
value *sgt*	セキュリティ グループ タグ番号を指定します。

コマンド デフォルト

デフォルトは **security-group-tag none** です。つまり、この属性に設定されているセキュリティ グループ タグはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーションまたはユーザ名コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、VPN セッションのセキュリティ グループ タギングをサポートしています。外部 AAA サーバを使用するか、または、ローカル ユーザか VPN グループ ポリシーのセキュリティ グループ タグを設定することで、セキュリティ グループ タグ（SGT）を VPN セッションに割り当てることができます。さらに、レイヤ 2 イーサネット経由で、Cisco TrustSec システムを介してこのタグを伝搬することができます。AAA サーバが SGT を提供できない場合には、セキュリティ グループ タグをグループ ポリシーで利用したり、ローカル ユーザが利用したりすることができます。

次は、VPN ユーザに SGT を割り当てるための一般的なプロセスです。

1. ユーザは、ISE サーバを含む AAA サーバ グループを使用しているリモート アクセス VPN に接続します。
2. ASA が ISE に AAA 情報を要求します。この情報に SGT が含まれている場合があります。ASA は、ユーザのトンネル トラフィックに対する IP アドレスの割り当ても行います。
3. ASA が AAA 情報を使用してユーザを認証し、トンネルを作成します。
4. ASA が AAA 情報から取得した SGT と割り当て済みの IP アドレスを使用して、レイヤ 2 ヘッダー内に SGT を追加します。
5. SGT を含むパケットが Cisco TrustSec ネットワーク内の次のピア デバイスに渡されます。

AAA サーバの属性に、VPN ユーザに割り当てるための SGT が含まれていない場合、ASA はグループ ポリシーの SGT を使用します。グループ ポリシーに SGT が含まれていない場合は、タグ 0x0 が割り当てられます。

例

次に、グループ ポリシーの SGT 属性を設定する方法の例を示します。

```
ciscoasa(config-group-policy)# security-group-tag value 101
```

関連コマンド

コマンド	説明
show asp table cts sgt-map	データ パスに保持されている IP アドレス セキュリティ グループのテーブル マップ データベースから IP アドレス セキュリティ グループのテーブル マップ エントリを表示します。
show cts sgt-map	制御パスの IP アドレス セキュリティ グループ テーブル マネージャ エントリを表示します。

security-level

インターフェイスのセキュリティ レベルを設定するには、インターフェイス コンフィギュレーション モードで **security-level** コマンドを使用します。セキュリティ レベルをデフォルトに設定するには、このコマンドの **no** 形式を使用します。セキュリティ レベルを指定すると、高いセキュリティ レベルのネットワークと低いセキュリティ レベルのネットワークとの間の通信に追加の保護が設定され、高いセキュリティ レベルのネットワークが低いセキュリティ レベルのネットワークから保護されます。

security-level *number*

no security-level

構文の説明

number	0（最低）～ 100（最高）の整数。

デフォルト

デフォルトのセキュリティ レベルは 0 です。

インターフェイスに「inside」という名前を指定して、明示的にセキュリティ レベルを設定しないと、ASA によってセキュリティ レベルが 100 に設定されます（**nameif** コマンドを参照）。このレベルは必要に応じて変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**nameif** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン:一部のインスペクション エンジンは、セキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン:発信接続に対してのみ適用されます。
  - OraServ インスペクション エンジン:ホストのペア間に OraServ ポートへの制御接続が存在する場合は、ASA 経由での着信データ接続のみが許可されます。
- フィルタリング:HTTP(S) および FTP フィルタリングは、(高いレベルから低いレベルへの)発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。
- NAT コントロール:NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス(内部)上のホストから低いセキュリティ レベルのインターフェイス(外部)上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。
- **established** コマンド:このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

通常、同じセキュリティ レベルのインターフェイス間では通信できません。同じセキュリティ レベルのインターフェイス間で通信する場合は、**same-security-traffic** コマンドを参照してください。101 を超える通信インターフェイスを作成する必要がある場合や、2 つのインターフェイス間のトラフィックに同じ保護機能を適用する必要がある場合(同程度のセキュリティが必要な 2 つの部門がある場合など)に、2 つのインターフェイスに同じレベルを割り当てて、それらのインターフェイス間での通信を許可できます。

インターフェイスのセキュリティ レベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear local-host** コマンドを使用して接続をクリアできます。

例

次に、2 つのインターフェイスのセキュリティ レベルを 100 と 0 に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear local-host	すべての接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

segment-id

VNI インターフェイスの VXLAN ID を指定するには、インターフェイス コンフィギュレーション モードで **segment-id** コマンドを使用します。ID を削除するには、このコマンドの **no** 形式を使用します。

segment-id *id*

no segment-id *id*

構文の説明

id	1 ～ 16777215 の範囲で ID を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

セグメント ID は VXLAN タギングに使用されます。

例

次に、VNI 1 インターフェイスを設定し、1000 のセグメント ID を指定する例を示します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

send response

RADIUS の Accounting-Response Start および Accounting-Response Stop メッセージを RADIUS の Accounting-Request Start および Stop メッセージの送信元に送信するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **send response** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスします。

このオプションは、デフォルトで無効です。

send response

no send response

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、RADIUS アカウンティングで応答を送信する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# send response
ciscoasa(config-pmap-p)# send response
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
パラメータ	インスペクション ポリシー マップのパラメータを設定します。

seq-past-window

パストウィンドウ シーケンス番号（TCP 受信ウィンドウの適切な境界を越える受信 TCP パケットのシーケンス番号）を持つパケットに対するアクションを設定するには、tcp マップ コンフィギュレーション モードで **seq-past-window** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

seq-past-window {**allow** | **drop**}

no seq-past-window

構文の説明

allow	パストウィンドウ シーケンス番号を持つパケットを許可します。このアクションは、**queue-limit** コマンドが 0（ディセーブル）に設定されている場合に限り許可されます。
drop	パストウィンドウ シーケンス番号を持つパケットをドロップします。

デフォルト

デフォルトのアクションでは、パストウィンドウ シーケンス番号を持つパケットはドロップされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが追加されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **seq-past-window**：tcp マップ コンフィギュレーション モードでは、**seq-past-window** コマンドおよびその他数多くのコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。

3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、パストウィンドウ シーケンス番号を持つパケットを許可するように ASA を設定する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# seq-past-window allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシー内でトラフィックに適用するアクションを指定します。
queue-limit	順序が不正なパケットの制限を設定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

serial-number

登録時に、ASA のシリアル番号を証明書に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **serial-number** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

serial-number

no serial-number

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定では、シリアル番号は含まれません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に ASA のシリアル番号を含める例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# serial-number
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。

server（POP3、IMAP4、SMTP）（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

デフォルトの電子メール プロキシ サーバを指定するには、該当する電子メール プロキシ コンフィギュレーション モードで **server** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。ASA は、ユーザがサーバを指定せずに電子メール プロキシに接続した場合、デフォルトの電子メール サーバに要求を送信します。デフォルトのサーバを設定せず、ユーザもサーバを指定しない場合、ASA ではエラーが返されます。

server {*ipaddr or hostname*}

no server

構文の説明

hostname	デフォルトの電子メール プロキシ サーバの DNS 名。
ipaddr	デフォルトの電子メール プロキシ サーバの IP アドレス。

デフォルト

デフォルトでは、デフォルトの電子メール プロキシ サーバはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Pop3s コンフィギュレーション	• 対応	• 対応	—	—	• 対応
Imap4s コンフィギュレーション	• 対応	• 対応	—	—	• 対応
smtps コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5.2	このコマンドは廃止されました。

例

次に、IP アドレス 10.1.1.7 を指定してデフォルトの POP3S 電子メール サーバを設定する例を示します。

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# server 10.1.1.7
```

server（ScanSafe 汎用オプション）

プライマリおよびバックアップ クラウド Web セキュリティ プロキシ サーバを設定するには、ScanSafe 汎用オプション コンフィギュレーション モードで **server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。

server {**primary** | **backup**} {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

no server {**primary** | **backup**} {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

構文の説明

backup	バックアップ サーバを識別していることを指定します。
ip *ip_address*	サーバの IP アドレスを指定します。
fqdn *fqdn*	サーバの完全修飾ドメイン名（FQDN）を指定します。
port *port*	（オプション）デフォルトでは、クラウド Web セキュリティ プロキシ サーバは HTTP と HTTPS の両方のトラフィックにポート 8080 を使用します。指示されている場合以外は、この値を変更しないでください。
primary	プライマリ サーバを識別していることを指定します。

コマンド デフォルト

デフォルト ポートは 8080 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
scansafe 汎用オプション コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco Cloud Web Security サービスに登録すると、プライマリ クラウド Web セキュリティ プロキシ サーバとバックアップ プロキシ サーバが割り当てられます。これらのサーバは、アベイラビリティをチェックするために定期的にポーリングされます。ASA がクラウド Web セキュリティ プロキシ サーバに到達することができない場合（SYN/ACK パケットがプロキシ サーバから到着しない場合など）、プロキシ サーバは TCP スリーウェイ ハンドシェイクを介してポーリングされて、アベイラビリティがチェックされます。設定した試行回数（デフォルトは 5）後に、プロキシ サーバが使用不可の場合、サーバは到達不能として宣言され、バックアップ プロキシ サーバがアクティブになります。

(注) クラウド Web セキュリティ アプリケーションの状態をチェックすることで、フェールオーバーをさらに改善することができます。場合によっては、サーバが TCP スリーウェイ ハンドシェイクを完了できても、サーバ上のクラウド Web セキュリティ アプリケーションが正しく機能していないことがあります。アプリケーション健全性チェックを有効にすると、スリーウェイ ハンドシェイクが完了しても、アプリケーション自体が応答しない場合、システムはバックアップ サーバにフェールオーバーできます。これにより、より信頼性の高いフェールオーバー設定が確立されます。この追加のチェックを有効にするには、**health-check application** コマンドを使用します。

継続ポーリングによってプライマリ サーバが連続する 2 回の再試行回数の期間にアクティブであることが示されると、ASA はバックアップ サーバからプライマリ クラウド Web セキュリティ プロキシ サーバに自動的にフォール バックします。このポーリング間隔を変更するには、**retry-count** コマンドを使用します。

プロキシ サーバが到達可能でないトラフィック状態	サーバ タイムアウトの計算	接続タイムアウトの結果
トラフィックが多い	クライアントのハーフ オープンの接続のタイムアウト + ASA TCP 接続タイムアウト	(30 + 30)= 60 秒
単一接続の失敗	クライアントのハーフ オープンの接続のタイムアウト + ((再試行しきい値 - 1)x(ASA TCP 接続タイムアウト))	(30 +((5-1)x(30)))= 150 秒
アイドル:接続は送信されていません。	15 分 +((再試行しきい値)x (ASA TCP 接続タイムアウト))	900 +(5 x(30))= 1050 秒

例

次に、プライマリ サーバとバックアップ サーバを設定する例を示します。プライマリ サーバおよびバックアップ サーバに対して個別にコマンドを入力する必要があります。

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
health-check application	フェールオーバーのための、クラウド Web セキュリティのアプリケーション健全性チェックを有効にします。
http[**s**](パラメータ)	インスペクション ポリシー マップのサービス タイプ(HTTP または HTTPS)を指定します。

コマンド	説明
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の HTTP 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

server (ssh pubkey-chain)

オンボードのセキュア コピー(SCP)クライアントの SSH サーバおよびそのキーを ASA データベースに対して手動で追加または削除するには、ssh pubkey-chain コンフィギュレーション モードで **server** コマンドを使用します。サーバおよびそのホスト キーを削除するには、このコマンドの **no** 形式を使用します。

server *ip_address*

no server *ip_address*

構文の説明

ip_address	SSH サーバの IP アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ssh pubkey-chain コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

オンボードの SCP クライアントを使用して、ASA との間でファイルをコピーすることができます。ASA は接続先の各 SCP サーバの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバとそのキーを追加または削除できます。

各サーバについて、SSH ホストの **key-string**(公開キー) または **key-hash**(ハッシュ値)を指定できます。

例

次に、10.86.94.170 にあるサーバのすでにハッシュされているホスト キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

次に、10.7.8.9 にあるサーバのホスト ストリング キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

関連コマンド

コマンド	説明
copy	ASA との間でファイルをコピーします。
key-hash	ハッシュ SSH ホスト キーを入力します。
key-string	公開 SSH ホスト キーを入力します。
ssh pubkey-chain	ASA のデータベースに格納されるサーバとそのキーを手動で追加または削除します。
ssh stricthostkeycheck	オンボードのセキュア コピー(SCP)クライアントの SSH ホスト キーのチェックをイネーブルにします。

server authenticate-client

TLS ハンドシェイク時における ASA での TLS クライアントの認証をイネーブルにするには、TLS プロキシ コンフィギュレーション モードで **server authenticate-client** コマンドを使用します。

クライアント認証をバイパスするには、このコマンドの **no** 形式を使用します。

server authenticate-client

no server authenticate-client

構文の説明

このコマンドには、引数またはキーワードがありません。

デフォルト

このコマンドは、デフォルトでイネーブルです。つまり、ASA とのハンドシェイク時に、TLS クライアントは、証明書の提示を要求されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

TLS プロキシ ハンドシェイク時にクライアント認証が必要であるかどうかを制御するには、**server authenticate-client** コマンドを使用します。イネーブルの場合（デフォルト）、セキュリティ アプライアンスは TLS クライアントに証明書要求 TLS ハンドシェイク メッセージを送信し、TLS クライアントは証明書の提示を要求されます。

クライアント認証をディセーブルにするには、このコマンドの **no** 形式を使用します。TLS クライアント認証のディセーブルは、ASA が CUMA クライアントや、Web ブラウザなどのクライアント証明書を送信できないクライアントと相互運用する必要がある場合に適しています。

例

次に、クライアント認証をディセーブルにした TLS プロキシ インスタンスを設定する例を示します。

```
ciscoasa(config)# tls-proxy mmp_tls
ciscoasa(config-tlsp)# no server authenticate-client
ciscoasa(config-tlsp)# server trust-point cuma_server_proxy
```

関連コマンド

コマンド	説明
tls-proxy	TLS プロキシ インスタンスを設定します。

server cipher-suite

TLS プロキシ サーバで使用できる暗号方式を定義するには、tls プロキシ コンフィギュレーション モードで **server cipher suite** コマンドを使用します。グローバルな暗号方式の設定を使用するには、このコマンドの **no** 形式を使用します。

server cipher-suite *cipher_list*

no server cipher-suite *cipher_list*

構文の説明

cipher_list	次の任意の組み合わせを含めるように暗号方式を設定します。 • **3des-sha1** • **aes128-sha1** • **aes256-sha1** • **des-sha1** • **null-sha1** • **rc4-sha1** 複数のオプションはスペースで区切ります。

コマンド デフォルト

TLS プロキシで使用できる暗号方式を定義しないと、プロキシ サーバは **ssl cipher** コマンドによって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルは medium です。つまり、NULL-SHA、DES-CBC-SHA、および RC4-MD5 を除くすべての暗号方式が使用できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。

使用上のガイドライン

ASA が TLS プロキシ サーバとして動作している場合は、SSL 暗号スイートを設定できるようになりました。以前は、ASA に グローバル設定を行うには、**ssl cipher** コマンドを使用するしかありませんでした。

ASA で一般的に使用可能なスイート（**ssl cipher** コマンド）以外の別のスイートを使用する場合にのみ、server cipher-suite コマンドを指定します。

ASA 上のすべての SSL サーバ接続に最小 TLS バージョンを設定する場合は、**ssl server-version** コマンドを参照してください。デフォルトは TLS v1.0 です。

例

次に、TLS プロキシ サーバ暗号方式を設定する例を示します。

```
ciscoasa(config)# tls-proxy test
ciscoasa(config-tlsp)# server cipher-list aes128-sha1 aes256-sha1
```

関連コマンド

コマンド	説明
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。
client cipher-list	TLS プロキシ クライアントの暗号スイートを定義します。

server-port

ホストの AAA サーバ ポートを設定するには、AAA サーバ ホスト モードで **server-port** コマンドを使用します。指定されているサーバ ポートを削除するには、このコマンドの **no** 形式を使用します。

server-port *port-number*

no server-port *port-number*

構文の説明

port-number	0 ～ 65535 の範囲のポート番号。

デフォルト

デフォルトのサーバ ポートは次のとおりです。

- SDI：5500
- LDAP：389
- Kerberos：88
- NT：139
- TACACS+：49

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ グループ	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、srvgrp1 という名前の SDI AAA サーバでサーバ ポート番号 8888 を使用するように設定する例を示します。

```
ciscoasa(config)# aaa-server srvgrp1 protocol sdi
ciscoasa(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
ciscoasa(config-aaa-server-host)# server-port 8888
```

関連コマンド

コマンド	説明
aaa-server host	ホスト固有の AAA サーバ パラメータを設定します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

server-separator（POP3、IMAP4、SMTP）（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

電子メール サーバ名および VPN サーバ名のデリミタとして文字を指定するには、該当する電子メール プロキシ モードで **server-separator** コマンドを使用します。デフォルト（「:」）に戻すには、このコマンドの no 形式を使用します。

server-separator {*symbol*}

no server-separator

構文の説明

シンボル	電子メール サーバ名および VPN サーバ名を区切る文字。使用できるのは、「@」（アットマーク）、「|」（パイプ）、「:」（コロン）、「#」（番号記号）、「,」（カンマ）、および「;」（セミコロン）です。

デフォルト

デフォルトは「@」（アット マーク）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
pop3s	• 対応	—	• 対応	—	—
Imap4s	• 対応	—	• 対応	—	—
Smtps	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5.2	このコマンドは廃止されました。

使用上のガイドライン

サーバの区切り文字には、名前の区切り文字とは異なる文字を使用する必要があります。

例

次に、パイプ（|）を IMAP4S サーバの区切り文字として設定する例を示します。

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# server-separator |
```

関連コマンド

コマンド	説明
name-separator	電子メールおよび VPN のユーザ名とパスワードを区切ります。

server trust-point

TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定するには、TLS サーバ コンフィギュレーション モードで **server trust-point** コマンドを使用します。

server trust-point *proxy_trustpoint*

構文の説明

proxy_trustpoint	**crypto ca trustpoint** コマンドによって定義されるトラストポイントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントでは、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。**server trust-point** コマンドは、グローバル **ssl trust-point** コマンドよりも優先されます。

server trust-point コマンドは、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定します。証明書は、ASA が所有している必要があります（ID 証明書）。証明書には、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。

接続を開始できる各エンティティに対して TLS プロキシ インスタンスを作成します。TLS 接続を開始するエンティティは、TLS クライアントのロールを担います。TLS プロキシにはクライアント プロキシとサーバ プロキシが厳密に定義されているため、いずれのエンティティからも接続が開始される可能性がある場合には、2 つの TLS プロキシ インスタンスを定義する必要があります。

（注） 電話プロキシとともに使用する TLS プロキシ インスタンスを作成する場合、サーバのトラストポイントは、CTL ファイル インスタンスによって作成される内部電話プロキシ トラストポイントです。トラストポイント名は、*internal_PP_<ctl-file_instance_name> の形式となります。*

例

次に、**server trust-point** コマンドを使用して、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定する例を示します。

```
ciscoasa(config-tlsp)# server trust-point ent_y_proxy
```

関連コマンド

コマンド	説明
client (tls-proxy)	TLS プロキシ インスタンスのトラストポイント、キー ペア、および暗号スイートを設定します。
client trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。
tls-proxy	TLS プロキシ インスタンスを設定します。

server-type

LDAP サーバ モデルを手動で設定するには、AAA サーバ ホスト コンフィギュレーション モードで **server-type** コマンドを使用します。ASA では、次のサーバ モデルがサポートされています。

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server（以前の Sun ONE Directory Server）
- LDAPv3 に準拠した一般的な LDAP ディレクトリ サーバ（パスワード管理なし）

このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

no server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

構文の説明

auto-detect	ASA で自動検出によって LDAP サーバ タイプを決定することを指定します。
generic	Sun および Microsoft の LDAP ディレクトリ サーバ以外の LDAP v3 準拠のディレクトリ サーバを指定します。一般的な LDAP サーバでは、パスワード管理はサポートされません。
microsoft	LDAP サーバが Microsoft Active Directory であることを指定します。
openldap	LDAP サーバが OpenLDAP サーバであることを指定します。
novell	LDAP サーバが Novell サーバであることを指定します。
sun	LDAP サーバが Sun Microsystems JAVA System Directory Server であることを指定します。

デフォルト

デフォルトでは、自動検出によってサーバ タイプの決定が試みられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.0(2)	OpenLDAP および Novell サーバ タイプのサポートが追加されました。

使用上のガイドライン

ASA は LDAP バージョン 3 をサポートしており、Sun Microsystems JAVA System Directory Server、Microsoft Active Directory、およびその他の LDAPv3 ディレクトリ サーバと互換性があります。

（注）

- Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- Microsoft：Microsoft Active Directory でパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。
- Generic：パスワード管理機能はサポートされていません。

デフォルトで、ASA では、Microsoft ディレクトリ サーバ、Sun LDAP ディレクトリ サーバ、または一般的な LDAPv3 サーバのいずれに接続しているかが自動検出されます。ただし、自動検出で LDAP サーバ タイプを決定できない場合で、サーバが Microsoft または Sun のサーバであることが明らかである場合は、**server-type** コマンドを使用して、サーバを Microsoft または Sun Microsystems の LDAP サーバとして手動で設定できます。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、IP アドレス 10.10.0.1 の LDAP サーバ ldapsvr1 のサーバ タイプを設定する例を示します。この最初の例では、Sun Microsystems LDAP サーバを設定しています。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type sun
```

次に、ASA で自動検出を使用してサーバ タイプを決定することを指定する例を示します。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol LDAP
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type auto-detect
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL が LDAP クライアントとサーバ間の接続を保護することを指定します。
sasl-mechanism	LDAP クライアントおよびサーバ間での SASL 認証を設定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

service (ctl-provider)

証明書信頼リスト プロバイダーがリッスンするポートを指定するには、CTL プロバイダー コンフィギュレーション モードで **service** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

service port *listening_port*

no service port *listening_port*

構文の説明

port *listening_port*	クライアントにエクスポートする証明書を指定します。

デフォルト

デフォルトのポートは 2444 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ctl プロバイダー コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CTL プロバイダーがリッスンするポートを指定するには、CTL プロバイダー コンフィギュレーション モードで **service** コマンドを使用します。ポートは、クラスタ内の CallManager サーバによってリッスンされているポートである必要があります（[CallManager administration] ページの [Enterprise Parameters] で設定）。デフォルトのポートは 2444 です。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
クライアント	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードも指定します。
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

service（グローバル）

拒否された TCP 接続のリセットをイネーブルにするには、グローバル コンフィギュレーション モードで **service** コマンドを使用します。リセットをディセーブルにするには、このコマンドの **no** 形式を使用します。

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

構文の説明

interface *interface_name*	指定したインターフェイスのリセットをイネーブルまたはディセーブルにします。
resetinbound	ASA の通過を試み、アクセス リストまたは AAA 設定に基づいて ASA によって拒否されたすべての着信 TCP セッションに TCP リセットを送信します。ASA は、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。インターフェイスを指定しない場合、この設定はすべてのインターフェイスに適用されます。
resetoutbound	ASA の通過を試み、アクセス リストまたは AAA 設定に基づいて ASA によって拒否されたすべての発信 TCP セッションに TCP リセットを送信します。ASA は、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。このオプションは、デフォルトで有効です。たとえば、トラフィック ストーム時に CPU の負荷を軽減するためなどに発信リセットをディセーブルにできます。
resetoutside	最もセキュリティ レベルの低いインターフェイスで終端し、アクセス リストまたは AAA 設定に基づいて ASA によって拒否された TCP パケットのリセットをイネーブルにします。ASA は、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。このオプションをイネーブルにしなかった場合、ASA は拒否されたパケットを何も通知せずに廃棄します。 インターフェイス PAT では、**resetoutside** キーワードを使用することを推奨します。このキーワードを使用すると、外部 SMTP または FTP サーバからの IDENT を ASA で終了できます。これらの接続をアクティブにリセットすることによって、30 秒のタイムアウト遅延を回避できます。 **（注）** 接続はこのオプションに関係なく、常に BGP と WebVPN（安全性が最低のインターフェイス）にリセットされます。

デフォルト

デフォルトでは、すべてのインターフェイスで **service resetoutbound** がイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	**interface** キーワードおよび **resetoutbound** コマンドが追加されました。

使用上のガイドライン

アイデンティティ要求（IDENT）接続をリセットする必要がある場合は、着信トラフィックに対して明示的にリセットを送信できます。拒否されたホストに TCP RST（TCP ヘッダーのリセットフラグ）を送信すると、RST によって着信 IDENT プロセスが停止されるため、IDENT がタイムアウトするのを待機する必要がなくなります。外部ホストは IDENT がタイムアウトするまで SYN を継続的に再送信するため、IDENT がタイムアウトするのを待機するとトラフィックの速度低下の原因となる可能性があります。そのため、**service resetinbound** コマンドによってパフォーマンスが向上する可能性があります。

例

次に、内部インターフェイスを除くすべてのインターフェイスで発信リセットをディセーブルにする例を示します。

```
ciscoasa(config)# no service resetoutbound
ciscoasa(config)# service resetoutbound interface inside
```

次に、DMZ インターフェイスを除くすべてのインターフェイスで着信リセットをイネーブルにする例を示します。

```
ciscoasa(config)# service resetinbound
ciscoasa(config)# no service resetinbound interface dmz
```

次に、外部インターフェイスが終端となる接続でリセットをイネーブルにする例を示します。

```
ciscoasa(config)# service resetoutside
```

関連コマンド

コマンド	説明
show running-config service	サービス コンフィギュレーションを表示します。

service（オブジェクト サービス）

サービス オブジェクトのプロトコルおよびオプションの属性を定義するには、オブジェクト サービス コンフィギュレーション モードで **service** コマンドを使用します。定義を削除するには、このコマンドの **no** 形式を使用します。

service {*protocol* | {**tcp** | **udp** | **sctp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]}

no service {*protocol* | {**tcp** | **udp** | **sctp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]}

構文の説明

destination *operator number*	（オプション：**tcp**、**udp**、**sctp** のみ）宛先ポート名または番号（0 ～ 65535）を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は次のとおりです。 • **eq**：ポート番号に等しい。 • **gt**：ポート番号より大きい。 • **lt**：ポート番号より小さい。 • **neq**：ポート番号と等しくない。 • **range**：ポート範囲。2 つの番号は、**range 1024 4500** のようにスペースで区切って指定します。
{**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]	サービス タイプが ICMP または ICMP バージョン 6 接続用であることを指定します。任意で ICMP タイプを名前または番号（0 ～ 255）で指定できます（使用可能なオプションの ICMP タイプ名については、CLI のヘルプを参照してください）。タイプを指定すると、オプションで ICMP コード（1 ～ 255）を含めることができます。
protocol	プロトコル名または番号（0 ～ 255）を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。
sctp	サービス タイプが Stream Control Transmission Protocol（SCTP）接続であることを指定します。
source *operator number*	（オプション：**tcp**、**udp**、**sctp** のみ）送信元ポート名または番号（0 ～ 65535）を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は **destination** のものと同じです。
tcp	サービス タイプが TCP 接続用であることを指定します。
udp	サービス タイプが UDP 接続用であることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
オブジェクト サービス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.0(1)	ICMP コードのサポートが追加されました。
9.5(2)	SCTP のサポートが追加されました。

使用上のガイドライン

ACL（**access-list** コマンド）や NAT（**nat** コマンド）など、コンフィギュレーションの他の部分ではサービス オブジェクトを名前で使用できます。

既存のサービス オブジェクトを別のプロトコルおよびポートを使用して設定した場合、新しいコンフィギュレーションでは既存のプロトコルとポートが新しいプロトコルとポートに置き換わります。

例

次に、SSH トラフィックのサービス オブジェクトを作成する例を示します。

```
ciscoasa(config)# object service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
```

次に、EIGRP トラフィックのサービス オブジェクトを作成する例を示します。

```
ciscoasa(config)# object service EIGRP
ciscoasa(config-service-object)# service eigrp
```

次に、ポート 0 ～ 1024 から HTTPS へのトラフィックに対してサービス オブジェクトを作成する例を示します。

```
ciscoasa(config)# object service HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
object-group service	サービス オブジェクトを設定します。
show running-config object service	現在のサービス オブジェクト コンフィギュレーションを表示します。

service call-home

Call Home サービスをイネーブルにするには、グローバル コンフィギュレーション モードで **service call-home** コマンドを使用します。Call Home サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

service call-home

no service call-home

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトで、サービス Call Home コマンドはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

例

次に、Call Home サービスをイネーブルにする例を示します。

```
ciscoasa(config)# service call-home
```

次に、Call Home サービスをディセーブルにする例を示します。

```
hostname(config)# no service call-home
```

関連コマンド

コマンド	説明
call-home（グローバル コンフィギュレーション）	Call Home コンフィギュレーション モードを開始します。
call-home test	Call Home テスト メッセージを手動で送信します。
show call-home	Call Home コンフィギュレーション情報を表示します。

service-module

サービスモジュールが応答しなくなったことをシステムが判断するまでの時間を調整するには、グローバル コンフィギュレーション モードで **service-module** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

service-module {*module_id* | **all**} {**keepalive-counter** | **keepalive-timeout**} *value*

no service-module {*module_id* | **all**} {**keepalive-counter** | **keepalive-timeout**} *value*

構文の説明

{*module_id* | **all**}	キープアライブ値を調整するモジュールを指定します。**all** を指定すると、すべてのモジュールのキープアライブ値を調整します。**?** を使用して、システムに有効なモジュール ID を決定します。ID は通常、次のようになります。 • 最初のスロットのモジュールの場合は **1**。 • ASA FirePOWER モジュールの場合は **sfr**。
keepalive-counter *value*	モジュールがダウンしていると見なされる前に応答なしで送信できるキープアライブの最大数（1 ～ 12）。
keepalive-timeout *value*	キープアライブメッセージの送信間隔（4 ～ 16 秒）。

デフォルト

デフォルトのカウントは 6、デフォルトのタイムアウトは 4 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.12(3)	このコマンドが追加されました。

使用上のガイドライン

システムでは、コントロールプレーンのキープアライブメッセージを送信することで、サービスモジュールのヘルスステータスを定期的にチェックしています。CPU の使用率が高いために通信の遅延が発生した場合、システムが応答をすぐに受信できず、これによりモジュールから応答を受信しなかったと判断する可能性があります。システムは、モジュールが実際には正常に機能しているにもかかわらず、ダウンしていることを宣言し、通信チャネルを閉じます。ハイアベイラビリティが設定されている場合、システムはサービスカードの障害によりバックアップユニットにフェールオーバーします。これがセットアップ中頻繁に発生する場合は、キープアライブ時間を延長するか、システムがモジュールの障害を宣言するまでの時間を延長してください。

例

次の例では、キープアライブ時間およびタイムアウトを変更する方法について示します。

```
ciscoasa(config)# service-module all keepalive-count 10
ciscoasa(config)# service-module all keepalive-timeout 8
```

service-object

TCP、UDP、または TCP-UDP として事前定義されていないサービスまたはサービス オブジェクトをサービス オブジェクト グループに追加するには、オブジェクトグループ サービス コンフィギュレーション モードで **service-object** コマンドを使用します。サービスを削除するには、このコマンドの **no** 形式を使用します。

service-object {*protocol* | {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]] | **object** *name*}

no service-object {*protocol* | {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]] | **object** *name*}

構文の説明

destination *operator number*	(オプション:**tcp**、**udp**、**tcp-udp**、**sctp** のみ)宛先ポート名または番号(0 ～ 65535)を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は次のとおりです。 • **eq**:ポート番号に等しい。 • **gt**:ポート番号より大きい。 • **lt**:ポート番号より小さい。 • **neq**:ポート番号と等しくない。 • **range**:ポート範囲。2 つの番号は、**range 1024 4500** のようにスペースで区切って指定します。
{**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]	サービス タイプが ICMP または ICMP バージョン 6 接続用であることを指定します。任意で ICMP タイプを名前または番号(0 ～ 255)で指定できます(使用可能なオプションの ICMP タイプ名については、CLI のヘルプを参照してください)。タイプを指定すると、オプションで ICMP コード(1 ～ 255)を含めることができます。
object *name*	名前付きオブジェクトまたはグループをオブジェクトに追加します。
protocol	プロトコル名または番号(0 ～ 255)を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。
sctp	サービス タイプが Stream Control Transmission Protocol(SCTP)接続であることを指定します。
source *operator number*	(オプション:**tcp**、**udp**、**tcp-udp**、**sctp** のみ)送信元ポート名または番号(0 ～ 65535)を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は **destination** のものと同じです。
tcp	サービス タイプが TCP 接続用であることを指定します。
tcp-udp	サービス タイプが TCP または UDP 接続用であることを指定します。
udp	サービス タイプが UDP 接続用であることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
オブジェクトグループ サービス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(1)	このコマンドが追加されました。
8.3(1)	**object** キーワードが、サービス オブジェクト（**object service** コマンド）をサポートするために追加されました。
9.0(1)	ICMP コードのサポートが追加されました。
9.5(2)	SCTP のサポートが追加されました。

使用上のガイドライン

object-group service コマンドを使用してサービス オブジェクト グループを作成した場合、グループ全体に対してプロトコル タイプを事前定義していなければ、**service-object** コマンドを使用して、複数のサービスおよびサービス オブジェクト（ポートを含む）をさまざまなプロトコルのグループに追加できます。**object-group service [tcp | udp | tcp-udp]** コマンドを使用して特定のプロトコル タイプに対してサービス オブジェクト グループを作成した場合、**port-object** コマンドを使用してオブジェクト グループに指定できるのは宛先ポートのみです。

例

次の例では、TCP と UDP の両方のサービスを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

次の例では、複数のサービス オブジェクトを同じサービス オブジェクト グループに追加する方法を示します。

```
hostname(config)# service object SSH
hostname(config-service-object)# service tcp destination eq ssh

hostname(config)# service object EIGRP
hostname(config-service-object)# service eigrp

hostname(config)# service object HTTPS
hostname(config-service-object)# service tcp source range 0 1024 destination eq https

ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# service-object object SSH
ciscoasa(config-service-object-group)# service-object object EIGRP
ciscoasa(config-service-object-group)# service-object object HTTPS
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object service	サービス オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

service password-recovery

パスワードの回復をイネーブルにするには、グローバル コンフィギュレーション モードで **service password-recovery** コマンドを使用します。パスワードの回復をディセーブルにするには、このコマンドの **no** 形式を使用します。パスワードの回復はデフォルトでイネーブルですが、不正なユーザがパスワードの回復メカニズムを使用して ASA を侵害できないようにするためにディセーブルにすることができます。

service password-recovery

no service password-recovery

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

パスワードの回復は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、パスワードを忘れた場合、起動時にプロンプトが表示されたときに端末のキーボードで Esc キーを押して、ROMMON で ASA を起動できます。次に、コンフィギュレーション レジスタを変更することによって、スタートアップ コンフィギュレーションを無視するように ASA を設定します（**config-register** コマンドを参照）。たとえば、コンフィギュレーション レジスタがデフォルトの 0x1 の場合、**confreg 0x41** コマンドを入力して値を 0x41 に変更します。ASA がリロードされると、デフォルトのコンフィギュレーションがロードされ、デフォルトのパスワードを使用して特権 EXEC モードを開始できます。その後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーしてスタートアップ コンフィギュレーションをロードし、パスワードをリセットします。最後に、コンフィギュレーション レジスタを元の設定に戻して、以前と同様に起動するように ASA を設定します。たとえば、グローバル コンフィギュレーション モードで **config-register 0x1** コマンドを入力します。

PIX 500 シリーズ セキュリティ アプライアンスでは、起動時にプロンプトが表示されたときに端末のキーボードで Esc キーを押して、モニタ モードで ASA を起動します。その後、PIX パスワード ツールを ASA にダウンロードして、すべてのパスワードおよび **aaa authentication** コマンドを消去します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザが ROMMON を開始することを防止でき、コンフィギュレーションも変更されないままとすることができます。ユーザが ROMMON を開始すると、ユーザは、ASA によって、すべてのフラッシュ ファイル システムを消去するように求められます。ユーザは、最初に消去を実行しないと、ROMMON を開始できません。ユーザがフラッシュ ファイル システムを消去しない場合、ASA はリロードします。パスワードの回復は ROMMON の使用と既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル(使用可能な場合)をロードします。**service password-recovery** コマンドは、コンフィギュレーション ファイルに情報提供の目的でのみ表示されます。CLI プロンプトでこのコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。ASA が起動時にスタートアップ コンフィギュレーションを無視するように設定されている場合にパスワードの回復をディセーブルにすると、ASA によって設定が変更され、通常どおりにスタートアップ コンフィギュレーションが起動されます。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password recovery** コマンドでスタンバイ装置に複製したときにコンフィギュレーション レジスタに同じ変更が加えられます。

PIX 500 シリーズ セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザは、PIX パスワード ツールによって、すべてのフラッシュ ファイル システムを消去するように求められます。ユーザは、最初に消去を実行しないと、PIX パスワード ツールを使用できません。ユーザがフラッシュ ファイル システムを消去しない場合、ASA はリロードします。パスワードの回復は既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル(使用可能な場合)をロードします。

例

次に、ASA 5500 シリーズのパスワードの回復をディセーブルにする例を示します。

```
ciscoasa(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON. The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images. You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

次に、ASA 5500 シリーズで、起動時に ROMMON を開始するタイミングとパスワードの回復操作を完了する例を示します。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
```

```
Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa# configure terminal
ciscoasa(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
ciscoasa(config)# enable password NewPassword
ciscoasa(config)# config-register 0x1
```

関連コマンド

コマンド	説明
config-register	リロード時にスタートアップ コンフィギュレーションを無視するように ASA を設定します。
イネーブル パスワード	イネーブル パスワードを設定します。
password	ログイン パスワードを設定します。

service-policy（クラス）

別のポリシー マップの下に階層型ポリシー マップを適用するには、クラス コンフィギュレーション モードで **service-policy** コマンドを使用します。サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。階層型ポリシーは、シェーピングされたトラフィックのサブセットに対してプライオリティ キューイングを実行する場合に QoS トラフィック シェーピングでのみサポートされています。

service-policy *policymap_name*

no service-policy *policymap_name*

構文の説明

policymap_name	**policy-map** コマンドで設定したポリシー マップ名を指定します。**priority** コマンドを含むレイヤ 3/4 ポリシー マップのみを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが追加されました。

使用上のガイドライン

階層型プライオリティ キューイングは、トラフィック シェーピング キューを有効にするインターフェイスで使用します。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キュー（**priority-queue** コマンド）は使用しません。

階層型プライオリティ キューイングでは、モジュラ ポリシー フレームワークを使用して次のタスクを実行します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**（プライオリティ キューイングの場合）：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **priority**：クラス マップのプライオリティ キューイングを有効にします。ポリシー マップを階層的に使用する場合は、このポリシー マップに priority コマンドだけを含めることができます。

3. **policy-map**（トラフィック シェーピングの場合）：**class-default** クラス マップに関連付けるアクションを指定します。
   a. **class class-default**：アクションを実行する **class-default** クラス マップを指定します。
   b. **shape**：トラフィック シェーピングをクラス マップに適用します。
   c. **service-policy**：プライオリティ キューイングをシェーピングされたトラフィックのサブセットに適用できるように、**priority** コマンドを設定したプライオリティ キューイング ポリシー マップを呼び出します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次の例では、外部インターフェイスのすべてのトラフィックでトラフィック シェーピングをイネーブルにして、DSCP ビットが ef に設定された VPN tunnel-grp1 内のトラフィックにプライオリティを付けます。

```
ciscoasa(config)# class-map TG1-voice
ciscoasa(config-cmap)# match tunnel-group tunnel-grp1
ciscoasa(config-cmap)# match dscp ef

ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class TG1-voice
ciscoasa(config-pmap-c)# priority

ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy

ciscoasa(config-pmap-c)# service-policy shape_policy interface outside
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	ポリシー マップにクラス マップを指定します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	サービス ポリシーの統計情報をクリアします。
policy-map	クラス マップに対して実行するアクションを指定します。
priority	プライオリティ キューイングをイネーブルにします。
service-policy (global)	インターフェイスにポリシー マップを適用します。
shape	トラフィック シェーピングをイネーブルにします。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

service-policy (global)

すべてのインターフェイスでグローバルに、または特定のインターフェイスでポリシー マップをアクティブにするには、グローバル コンフィギュレーション モードで **service-policy** コマンドを使用します。サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。インターフェイスでポリシーのセットをイネーブルにするには、**service-policy** コマンドを使用します。

service-policy *policymap_name* [**global** | **interface** *intf*] [**fail-close**]

no service-policy *policymap_name* [**global** | **interface** *intf*] [**fail-close**]

構文の説明

fail-close	IPv6 トラフィックをサポートしていないアプリケーション インスペクションによってドロップされた IPv6 トラフィックに対して syslog（767001）を生成します。デフォルトでは、syslog が生成されません。
global	すべてのインターフェイスにポリシー マップを適用します。
interface *intf*	特定のインターフェイスにポリシー マップを適用します。
policymap_name	**policy-map** コマンドで設定したポリシー マップ名を指定します。レイヤ 3/4 ポリシー マップのみを指定できます。インスペクション ポリシー マップ（**policy-map type inspect**）は指定できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	**fail-close** キーワードが追加されました。

使用上のガイドライン

サービス ポリシーをイネーブルにするには、Modular Policy Framework を使用します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. *commands for supported features*：特定のクラス マップについて、QoS、アプリケーション インスペクション、CSC または AIP SSM、TCP 接続と UDP 接続の制限とタイムアウト、TCP 正規化など、さまざまな機能の多数のアクションを設定できます。各機能で使用可能なコマンドの詳細については、CLI 設定ガイドを参照してください。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、インスペクションのグローバル ポリシーがあり、TCP 正規化のインターフェイス ポリシーがある場合、インターフェイスに対してインスペクションと TCP 正規化の両方が適用されます。ただし、インスペクションのグローバル ポリシーがあり、インスペクションのインターフェイス ポリシーもある場合、そのインターフェイスにはインターフェイス ポリシーのインスペクションのみが適用されます。

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するグローバル ポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがトラフィックにグローバルに適用されます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルト サービス ポリシーには、次のコマンドが含まれています。

```
service-policy global_policy global
```

例

次に、外部インターフェイスで inbound_policy ポリシー マップをイネーブルにする例を示します。

```
ciscoasa(config)# service-policy inbound_policy interface outside
```

次のコマンドは、デフォルト グローバル ポリシーをディセーブルにし、他のすべての ASA インターフェイスで新しいポリシー new_global_policy をイネーブルにします。

```
ciscoasa(config)# no service-policy global_policy global
ciscoasa(config)# service-policy new_global_policy global
```

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	サービス ポリシーの統計情報をクリアします。
service-policy (class)	別のポリシー マップの下に階層型ポリシーを適用します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

service sw-reset-button

ASA 5506-X、5508-X、および 5516-X でリセット ボタンをイネーブルにするには、グローバル コンフィギュレーション モードで **service sw-reset-button** コマンドを使用します。リセット ボタンをディセーブルにするには、このコマンドの **no** 形式を使用します。

service sw-reset-button

no service sw-reset-button

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

service sw-reset-button は、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	コマンドが追加されました。

使用上のガイドライン

リセット ボタンは背面パネルにある小さな埋め込み型のボタンです。約 3 秒以上押すと ASA がリセットされ、次のリブート後に「出荷時」のデフォルト状態に戻ります。設定変数が工場出荷時デフォルトにリセットされます。ただし、フラッシュは削除されないため、ファイルは削除されません。

例

次に、ソフトウェア リセット ボタンをイネーブルにする例を示します。

```
ciscoasa(config)# service sw-reset-button
ciscoasa(config)# show sw-reset-button

Software Reset Button is configured.
```

次に、ソフトウェア リセット ボタンを無効にする例を示します。

```
ciscoasa(config)# no service sw-reset-button
ciscoasa(config)# show sw-reset-button

Software Reset Button is not configured.
```

関連コマンド

コマンド	説明
show running-config service	サービス コンフィギュレーションを表示します。

サービス テレメトリ

テレメトリ データ サービスが有効になっている場合、デバイス情報、CPU/メモリ/ディスク/帯域幅の使用率、ライセンスの使用状況、設定済み機能リスト、クラスタ/フェールオーバー情報、およびお客様の ASA デバイスに関する同様の情報が、FXOS を介して Cisco Security Services Exchange（SSE）に送信されます。サービスを有効にするには、グローバル コンフィギュレーション モードで **service telemetry** コマンドを使用します。テレメトリ サービスを無効にするには、このコマンドの **no** 形式を使用します。

service telemetry

no service telemetry

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、サービス テレメトリ コマンドは有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが導入されました。

使用上のガイドライン

ASA テレメトリ サービスは、ASA アプリケーションを実行している SSPXRU（FP9300 および FP4100）プラットフォームでサポートされています。

例

次に、テレメトリ サービスを有効化する例を示します。

```
ciscoasa(config)# service telemetry
```

次に、テレメトリ サービスを無効化する例を示します。

```
hostname(config)# no service telemetry
```

関連コマンド

コマンド	説明
show telemetry	テレメトリの設定とアクティビティに関連する過去 100 のイベントを表示します。また、最後に送信されたテレメトリ データとサンプルが JSON 形式で表示されます。

session

ASA からモジュール（IPS SSP や CSC SSM など）への Telnet セッションを確立して、モジュール CLI にアクセスするには、特権 EXEC モードで **session** コマンドを使用します。

session *id*

構文の説明

id	モジュール ID を指定します。 • 物理モジュール：**1**（スロット番号 1 の場合） • ソフトウェア モジュール、ASA FirePOWER：**sfr** • ソフトウェア モジュール、IPS：**ips** • ソフトウェア モジュール、ASA CX：**cxsc**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.6(1)	IPS SSP ソフトウェア モジュールに対して **ips** モジュール ID が追加されました。
9.1(1)	ASA CX モジュールのサポートが追加されました（**cxsc** キーワード）。
9.2(1)	ASA FirePOWER モジュールのサポートが追加されました（**sfr** キーワード）。

使用上のガイドライン

このコマンドは、モジュールがアップ状態である場合にのみ使用できます。ステート情報については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、または Ctrl+Shift+6 を押してから x キーを押します。

次のハードウェア モジュールでは **session 1** コマンドを使用できないことに注意してください。

- ASA CX
- ASA FirePOWER

例

次に、スロット 1 のモジュールへのセッションを確立する例を示します。

```
ciscoasa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

関連コマンド

コマンド	説明
debug session-command	セッションのデバッグ メッセージを表示します。

session console

ASA からソフトウェア モジュール（IPS SSP ソフトウェア モジュールなど）への仮想コンソール セッションを確立するには、特権 EXEC モードで **session console** コマンドを使用します。このコマンドは、コントロール プレーンがダウンしているために **session** コマンドを使用して Telnet セッションを確立できない場合に便利です。

session *id* **console**

構文の説明

id	モジュール ID を指定します。 • ASA FirePOWER モジュール：**sfr** • IPS モジュール：**ips** • ASA CX モジュール：**cxsc** • ASA 5506W-X ワイヤレス アクセス ポイント：**wlan**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	ASA CX モジュールのサポートが追加されました（**cxsc** キーワード）。
9.2(1)	ASA FirePOWER モジュールのサポートが追加されました（**sfr** キーワード）。
9.4(1)	ASA 5506W-X ワイヤレス アクセス ポイント（**wlan** キーワード）のサポートが追加されました。

使用上のガイドライン

セッションを終了するには、**Ctrl-Shift-6** を押してから x キーを押します。

このコマンドは、**Ctrl+Shift+6**、x がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。**Ctrl+Shift+6**、x は、モジュール コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況でモジュール コンソールを終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、モジュール コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。

代わりに **session** コマンドを使用します。

例

次に、IPS モジュールへのコンソール セッションを作成する例を示します。

```
ciscoasa# session ips console

Establishing console session with slot 1
Opening console session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-SHIFT-6 then x'.

sensor login: service
Password: test
```

次に、ワイヤレス アクセス ポイントへのコンソール セッションを作成する例を示します。

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is ‘CTRL-^X’

ap>
```

関連コマンド

コマンド	説明
session	モジュールへの Telnet セッションを開始します。
show module log console	コンソール ログ情報を表示します。

session do

ASA からモジュールへの Telnet セッションを確立し、コマンドを実行するには、特権 EXEC モードで **session do** コマンドを使用します。

session *id* **do** *command*

構文の説明

id	モジュール ID を指定します。 • 物理モジュール：**1**（スロット番号 1 の場合） • ソフトウェア モジュール、ASA FirePOWER：**sfr** • ソフトウェア モジュール、IPS：**ips** • ソフトウェア モジュール、ASA CX：**cxsc**
command	モジュールでコマンドを実行します。サポートされるコマンドは次のとおりです。 • **setup host ip** *ip_address*/*mask*,*gateway_ip*：管理 IP アドレスおよびゲートウェイを設定します。 • **get-config**：モジュール コンフィギュレーションを取得します。 • **password-reset**：モジュール パスワードをデフォルトにリセットします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.6(1)	IPS SSP ソフトウェア モジュールに対して **ips** モジュール ID が追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを含め、ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、モジュールがアップ状態である場合にのみ使用できます。ステート情報については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、または **Ctrl+Shift+6** を押してから X キーを押します。

例

次に、管理 IP アドレスを 10.1.1.2/24 に、デフォルト ゲートウェイを 10.1.1.1 に設定する例を示します。

```
ciscoasa# session 1 do setup host ip 10.1.1.2/24,10.1.1.1
```

関連コマンド

コマンド	説明
debug session-command	セッションのデバッグ メッセージを表示します。

session ip

モジュール（IPS SSP や CSC SSM など）にロギング IP アドレスを設定するには、特権 EXEC モードで **session ip** コマンドを使用します。

session *id* **ip** {**address** *address mask* | **gateway** *address*}

構文の説明

id	モジュール ID を指定します。 • 物理モジュール：**1**（スロット番号 1 の場合） • ソフトウェア モジュール、IPS：**ips**
address *address*	syslog サーバ アドレスを設定します。
gateway *address*	ゲートウェイを syslog サーバに設定します。
mask	サブネット マスクを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。
8.6(1)	IPS SSP ソフトウェア モジュールに対して **ips** モジュール ID が追加されました。

使用上のガイドライン

このコマンドは、モジュールがアップ状態である場合にのみ使用できます。ステート情報については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、または **Ctrl+Shift+6** を押してから X キーを押します。

例

次に、スロット 1 のモジュールへのセッションを確立する例を示します。

```
ciscoasa# session 1 ip address
```

関連コマンド

コマンド	説明
debug session-command	セッションのデバッグ メッセージを表示します。

set as-path

BGP ルートの自律システム パスを変更するには、ルートマップ コンフィギュレーション モードで **set as-path** コマンドを使用します。自律システム パスを変更しないようにするには、このコマンドの **no** 形式を使用します。

set as-path {**tag** | **prepend** *as-path-string*}

no set as-path {**tag** | **prepend** *as-path-string*}

構文の説明

as-path-string	AS_PATH 属性に付加する自律システムの番号。この引数の値の範囲は、1 ～ 65535 の有効な自律システム番号です。複数の値を入力できます。最大 10 個の AS 番号を入力できます。 自律システムの番号形式の詳細については、**router bgp** コマンドを参照してください。
prepend	ルート マップにより照合されたルートの自律システム パスに、キーワード **prepend** に続いて文字列を付加します。BGP のインバウンド ルート マップおよびアウトバウンド ルート マップに適用します。
tag	ルートのタグを自律システム パスに変換します。BGP にルートを再配布するときのみ適用されます。

デフォルト

自律システム パスは変更されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

最適なパス選択に影響を与える唯一のグローバル BGP メトリックは、自律システム パス長です。自律システム パスの長さを変えることで、BGP スピーカーは遠くのピアによる最適なパス選択に影響を与えます。

タグを自律システム パスに変換することで、このコマンドの **set as-path tag** のバリエーションにより、自律システム長を変更できます。**set as-path prepend** のバリエーションを使用すれば、任意の自律システム パス文字列を BGP ルートに「付加」できます。通常、ローカルな自律システム番号は複数回追加され、AS パス長が増します。

シスコが採用している 4 バイト自律システム番号では、自律システム番号の正規表現のマッチングおよび出力表示のデフォルトの形式として asplain（たとえば、65538）を使用していますが、RFC 5396 で定義されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドに続けて、**clear bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。

例

次に、再配布されたルートのタグを自律システム パスに変換する例を示します。

```
ciscoasa(config)# route-map set-as-path-from-tag
ciscoasa(config-route-map)# set as-path tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute ospf 109 route-map set-as-path-from-tag
```

次に、10.108.1.1 にアドバタイズされたすべてのルートに 100 100 100 を付加する例を示します。

```
ciscoasa(config)# route-map set-as-path
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set as-path prepend 100 100 100
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 route-map set-as-path out
```

関連コマンド

コマンド	説明
clear bgp	ハードまたはソフトの再設定を使用して BGP 接続をリセットします。
bgp asnotation dot	デフォルトの表示を変更し、ボーダー ゲートウェイ プロトコル（BGP）4 バイト自律システム番号の正規表現一致形式を、asplain 形式（10 進数の値）からドット付き表記にします。

set automatic-tag

自動的にタグ値を計算するには、ルートマップ コンフィギュレーション モードで set automatic-tag コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

set automatic-tag

no set automatic-tag

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

タグを設定する場合は、match 句を使用する必要があります（permit everything を指している場合でも）。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、**route-map** グローバル コンフィギュレーション コマンドと、match および set **route-map** コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準、つまり現在の **route-map** コマンドに再配布が許可される条件を指定します。set コマンドは、set 処理、つまり match コマンドで指定した基準を満たしている場合に実行する特定の再配布アクションを指定します。**no route-map** コマンドは、ルート マップを削除します。

set **route-map** コンフィギュレーション コマンドを使用すると、ルート マップのすべての一致基準が満たされたときに実行される再配布 set 処理を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

例

次に、ボーダー ゲートウェイ プロトコル（BGP）で学習されたルートのタグ値が自動的に計算されるように Cisco ASA ソフトウェアを設定する例を示します。

```
ciscoasa(config-route-map)# route-map tag
ciscoasa(config-route-map)# match as-path 10
iscoasa(config-route-map)# set automatic-tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# table-map tag
```

set community

BGP コミュニティ属性を設定するには、**set community** ルート マップ コンフィギュレーション コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

set community {*community-number* [**additive**] | [*well-known-community*] [**additive**] | **none**}

no set community

構文の説明

additive	(オプション)既存のコミュニティにコミュニティを追加します。
community-number	そのコミュニティ番号を指定します。有効な値は、1 ～ 4294967200、**no-export**、または **no-advertise** です。
none	(オプション)ルート マップを渡すプレフィックスからコミュニティ属性を削除します。
well-known-community	(オプション)次のキーワードを使用することにより、ウェルノウン コミュニティを指定できます。 • **internet** • **local-as** • **no-advertise** • **no-export**

デフォルト

BGP コミュニティ属性は存在しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

タグを設定する場合は、match 句を使用する必要があります(「permit everything」リストを指している場合でも)。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、route-map グローバル コンフィギュレーション コマンドと、**match** および **set** route-map コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、*一致基準*(現在の **route-map** コマンドで再配布が許可される条件)を指定します。**set** コマンドは、*set 処理*(**match** コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクション)を指定します。**no route-map** コマンドは、ルート マップを削除します。

set ルート マップ コンフィギュレーション コマンドは、ルート マップのすべての一致基準が満たされたときに実行される再配布 *set 処理*を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

例

次の例では、自律システム パス アクセス リスト 1 を通過するルートのコミュニティが 109 に設定されます。自律システム パス アクセス リスト 2 を通過するルートのコミュニティは、no-export(これらのルートがどの eBGP ピアにもアドバタイズされない)に設定されます。

```
ciscoasa(config-route-map)# set community 10
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set community 109
ciscoasa(config-route-map)# set community 20
ciscoasa(config-route-map)# match as-path 2
ciscoasa(config-route-map)# set community no-export
```

関連コマンド

コマンド	説明
match as-path	アクセス リストで指定されている BGP 自律システム パスを照合します。

set connection

ポリシー マップ内のトラフィック クラスに対して接続制限を指定するには、クラス コンフィギュレーション モードで **set connection** コマンドを使用します。これらの指定を削除して、無制限の接続数を許可するには、このコマンドの **no** 形式を使用します。

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

構文の説明

conn-max *n*	（TCP、UDP、SCTP）。許可する同時接続の最大数を 0 ～ 2000000 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。たとえば、同時接続を許可するように 2 つのサーバが設定されている場合、接続制限数は、設定されている各サーバに別々に適用されます。TCP 接続の場合、確立された接続のみに適用されます。 クラスに設定された場合、この引数では、クラス全体で許可される同時接続最大数が制限されます。この場合、1 つの攻撃ホストがすべての接続を使い果たし、クラスにおいてアクセス リストに一致する他のホストが使用できる接続がなくなる可能性があります。
embryonic-conn-max *n*	許可する同時 TCP 初期接続の最大数を 0 ～ 2000000 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。
per-client-embryonic-max *n*	クライアントごとに許可する同時 TCP 初期接続の最大数を 0 ～ 2000000 の範囲で設定します。クライアントは、ASA から（新規接続を作成する）接続の初期パケットを送信するホストとして定義されます。 **access-list** が **class-map** とともに使用され、この機能のトラフィックが照合される場合、初期接続制限は、アクセス リストに一致するすべてのクライアントの累積初期接続数ではなく、ホストごとに適用されます。デフォルトは 0 で、この場合は接続数が制限されません。このキーワードは、管理クラス マップでは使用できません。
per-client-max *n*	（TCP、UDP、SCTP）。クライアントごとに許可する同時接続最大数を 0 ～ 2000000 の範囲で設定します。クライアントは、ASA から（新規接続を作成する）接続の初期パケットを送信するホストとして定義されます。TCP 接続の場合、これには確立済み接続、ハーフオープン接続、ハーフクローズ接続が含まれます。 **access-list** が **class-map** とともに使用され、この機能のトラフィックが照合される場合、接続制限は、アクセス リストに一致するすべてのクライアントの累積接続数ではなく、ホストごとに適用されます。デフォルトは 0 で、この場合は接続数が制限されません。 このキーワードは、管理クラス マップでは使用できません。クラスに設定された場合、このキーワードでは、クラスにおいてアクセス リストに一致する各ホストに許可される同時接続最大数が制限されます。

random-sequence-number {enable | disable}	TCP シーケンス番号ランダム化をイネーブルまたはディセーブルにします。このキーワードは、管理クラス マップでは使用できません。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

conn-max、**embryonic-conn-max**、**per-client-embryonic-max**、および **per-client-max** の各パラメータの *n* のデフォルト値は、0（接続数の制限なし）です。

シーケンス番号ランダム化は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	**per-client-embryonic-max** キーワードおよび **per-client-max** キーワードが追加されました。
8.0(2)	このコマンドが、ASA への管理トラフィックにおいて、レイヤ 3/4 管理クラス マップでも使用できるようになりました。**conn-max** キーワードおよび **embryonic-conn-max** キーワードだけが使用可能です。
9.0(1)	最大接続数が 65535 から 2000000 に増えました。
9.5(2)	**conn-max** キーワードと **per-client-max** キーワードが SCTP、TCP および UDP に適用されるようになりました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用してこのコマンドを設定します。最初に、**class-map** コマンド（通過トラフィック）または **class-map type management** コマンド（管理トラフィック）を使用して、タイムアウトを適用するトラフィックを定義します。次に、**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラス マップを参照します。クラス コンフィギュレーション モードで、**set connection** コマンドを入力できます。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、CLI 設定ガイドを参照してください。

(注) ASA モデル上の CPU コア数によっては、同時接続および初期接続の最大数が、各コアによる接続の管理方法が原因で、設定されている数を超える場合があります。最悪の場合、ASA は最大 *n*-1 の追加接続および初期接続を許可します。ここで、*n* はコアの数です。たとえば、モデルに 4 つのコアがあり、6 つの同時接続および 4 つの初期接続を設定した場合は、各タイプで 3 つの追加接続を使用できます。ご使用のモデルのコア数を確認するには、**show cpu core** コマンドを入力します。

TCP 代行受信の概要

初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、クライアントあたりの制限値と初期接続の制限を利用して TCP 代行受信を開始します。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、ASA はサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。ASA がクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

TCP シーケンスのランダム化

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。ASA は、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- ASA で eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- ASA で接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

例

次に、**set connection** コマンドを使用して、同時接続最大数を 256 に設定し、TCP シーケンス番号ランダム化をディセーブルにする例を示します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
ciscoasa(config-pmap-c)#
```

複数のパラメータを指定してこのコマンドを入力することも、各パラメータを個別のコマンドとして入力することもできます。ASA は、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
ciscoasa(config-pmap-c)# set connection conn-max 600
ciscoasa(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection conn-max 600 embryonic-conn-max 50
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、例外として、ポリシー マップが service-policy コマンドで使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
show service-policy	サービス ポリシー設定を表示します。**set connection** コマンドを含むポリシーを表示するには、**set connection** キーワードを使用します。

set connection advanced-options

接続の詳細設定を行うには、クラス コンフィギュレーション モードで **set connection advanced-options** コマンドを使用します。オプションを削除するには、このコマンドの **no** 形式を使用します。

set connection advanced-options {*tcp_mapname* | **tcp-state-bypass** | **sctp-state-bypass** | **flow-offload**}

no set connection advanced-options {*tcp_mapname* | **tcp-state-bypass** | **sctp-state-bypass** | **flow-offload**}

構文の説明

flow-offload	ASA からオフロードし、直接 NIC に切り替える対象として、一致するフローを指定します。これにより、データセンターにおける大量のデータ フローのパフォーマンスが向上します。フロー オフロードは、FXOS 1.1.3 以上を稼働する Firepower 9300 シリーズまたは FXOS 1.1.4 以上を稼働する Firepower 4100 シリーズで使用可能です。 このオプションを動作させるには、事前にフロー オフロードを有効にしておく必要があります。**flow-offload enable** コマンドを使用します。
sctp-state-bypass	SCTP ステート バイパスを実装して、SCTP ステートフル インスペクションを無効にします。SCTP トラフィックはプロトコル準拠かどうかを検証されません。
tcp_mapname	**tcp-map** コマンドで作成された TCP マップの名前。TCP 正規化をカスタマイズするには、このオプションを使用します。
tcp-state-bypass	ネットワーク内で非対称ルーティングを使用している場合は、TCP ステート チェックをバイパスします。TCP ステート バイパスの使用方法の詳細およびガイドラインについては、後述の「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。すべての TCP 正規化オプション（TCP マップ内）にデフォルト設定がありますが、デフォルトで有効になっているオプションはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	**tcp-state-bypass** キーワードが追加されました。
9.5(2)	**sctp-state-bypass** キーワードが追加されました。
9.5(2)	**flow-offload** キーワードが追加されました。オプションには、Firepower eXtensible Operating System 1.1.3 以上が必要です。オプションは、Firepower 9300 シリーズで使用可能です。
9.6(1)	FXOS 1.1.4 以上を稼働する Firepower 4100 シリーズでフロー オフロードのサポートが追加されました。

使用上のガイドライン

TCP マップを使用して TCP 正規化をカスタマイズするには、モジュラ ポリシー フレームワークを使用します。

1. **tcp-map**：変更する場合は、対象の TCP 正規化アクションを指定します。
2. **class-map**：TCP 正規化アクションを実行するトラフィックを指定します。
3. **policy-map**：クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced options**：TCP マップまたは別のオプションをクラス マップに適用します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

TCP ステート バイパス：個別のデバイスを通過するアウトバウンド フローおよびインバンド フローを許可する

デフォルトで、ASA を通過するすべてのトラフィックは、適応型セキュリティ アルゴリズムを使用して検査され、セキュリティ ポリシーに基づいて許可またはドロップされます。ASA では、各パケットの状態（新規接続であるか、または確立済み接続であるか）がチェックされ、そのパケットをセッション管理パス（新規接続の SYN パケット）、ファスト パス（確立済みの接続）、またはコントロール プレーン パス（高度なインスペクション）に割り当てることによって、ファイアウォールのパフォーマンスが最大化されます。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーのあらゆる面の再検査を受けることなく ASA を通過できます。この機能によってパフォーマンスは最大になります。ただし、SYN パケットを使用してファスト パスにセッションを確立する方法、およびファスト パスで行われるチェック（TCP シーケンス番号など）が、非対称ルーティング ソリューションの障害となる場合があります。これは、接続の発信フローと着信フローの両方が同じ ASA を通過する必要があるためです。

たとえば、ある新しい接続が ASA 1 に開始されるとします。SYN パケットはセッション管理パスを通過し、接続のエントリが高速パス テーブルに追加されます。この接続の後続のパケットが ASA 1 を通過する場合、パケットは高速パスのエントリと一致して、通過します。しかし、後続のパケットが ASA 2 に到着すると、SYN パケットがセッション管理パスを通過していないために、高速パスにはその接続のエントリがなく、パケットはドロップされます。

アップストリーム ルータに非対称ルーティングが設定されており、トラフィックが 2 つの ASA を通過することがある場合は、特定のトラフィックに対して TCP ステート バイパスを設定できます。TCP ステート バイパスは、高速パスでのセッションの確立方法を変更し、高速パスのインスペクションをディセーブルにします。この機能では、UDP 接続の処理と同様の方法で TCP トラフィックが処理されます。指定されたネットワークと一致した非 SYN パケットが ASA に入った時点で高速パス エントリが存在しない場合、高速パスで接続を確立するために、そのパケットはセッション管理パスを通過します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

TCP ステート バイパスでサポートされていない機能

TCP ステート バイパスを使用するときは、次の機能はサポートされません。

- アプリケーション検査:アプリケーション検査では、着信および発信トラフィックの両方が同じ ASA を通過する必要があるため、TCP ステート バイパスではアプリケーション検査はサポートされません。
- AAA 認証セッション:ユーザがある ASA で認証される場合、他の ASA 経由で戻るトラフィックは、その ASA でユーザが認証されていないため、拒否されます。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号ランダム化:ASA では接続の状態が追跡されないため、これらの機能は適用されません。
- TCP 正規化:TCP ノーマライザはディセーブルです。
- SSM 機能:TCP ステート バイパスと、IPS や CSC などの SSM 上で実行されるアプリケーションを使用することはできません。

TCP ステート バイパスの NAT のガイドライン

変換セッションは ASA ごとに個別に確立されるので、TCP ステート バイパス トラフィック用に両方の ASA でスタティック NAT を設定してください。ダイナミック NAT を使用すると、ASA 1 でのセッションに選択されるアドレスが、ASA 2 でのセッションに選択されるアドレスと異なります。

TCP ステート バイパスの接続タイムアウトのガイドライン

リリース 9.10(1) 以降、特定の接続に 2 分間トラフィックがない場合、接続はタイムアウトします。このデフォルトは、**set connection timeout idle** コマンドを使用して上書きできます。通常の TCP 接続は、デフォルトで 60 分後にタイムアウトします。9.10(1) よりも前のリリースでは、TCP ステートバイパス接続で 60 分間のグローバルタイムアウト値を使用します。

例

次に、**set connection advanced-options** コマンドを使用して、localmap という名前の TCP マップの使用を指定する例を示します。

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config-cmap)# exit
ciscoasa(config)# tcp-map localmap
ciscoasa(config)# policy-map global_policy global
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection advanced-options localmap
ciscoasa(config-pmap-c)#
```

次に、TCP ステート バイパスのコンフィギュレーション例を示します。

```
ciscoasa(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

ciscoasa(config)# class-map tcp_bypass
ciscoasa(config-cmap)# description "TCP traffic that bypasses stateful firewall"
ciscoasa(config-cmap)# match access-list tcp_bypass

ciscoasa(config-cmap)# policy-map tcp_bypass_policy
ciscoasa(config-pmap)# class tcp_bypass
ciscoasa(config-pmap-c)# set connection advanced-options tcp-state-bypass

ciscoasa(config-pmap-c)# service-policy tcp_bypass_policy interface outside
```

次に、SCTP ステート バイパスの設定例を示します。

```
ciscoasa(config)# access-list sctp_bypass extended permit sctp
10.1.1.0 255.255.255.224 any

ciscoasa(config)# class-map sctp_bypass
ciscoasa(config-cmap)# description "SCTP traffic that bypasses stateful inspection"
ciscoasa(config-cmap)# match access-list sctp_bypass

ciscoasa(config-cmap)# policy-map sctp_bypass_policy
ciscoasa(config-pmap)# class sctp_bypass
ciscoasa(config-pmap-c)# set connection advanced-options sctp-state-bypass

ciscoasa(config-pmap-c)# service-policy sctp_bypass_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップにクラス マップを指定します。
class-map	サービス ポリシーで使用するクラス マップを作成します。
flow-offload	フロー オフロードを有効にします。
policy-map	クラス マップと 1 つ以上のアクションを関連付けるポリシー マップを設定します。
service-policy	インターフェイスにポリシー マップを割り当てます。
set connection timeout	接続タイムアウトを設定します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
tcp-map	TCP マップを作成します。

set connection decrement-ttl

ポリシー マップ内のトラフィック クラスにおいて存続可能時間の値をデクリメントするには、クラス コンフィギュレーション モードで **set connection decrement-ttl** コマンドを使用します。存続可能時間をデクリメントしない場合は、このコマンドの **no** 形式を使用します。

set connection decrement-ttl

no set connection decrement-ttl

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトで、ASA では、存続可能時間はデクリメントされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンド、および **icmp unreachable** コマンドは、ASA をホップの 1 つとして表示する ASA 経由の traceroute を可能とするために必要です。

パケット存続時間（TTL）をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、パケット存続時間（TTL）をデクリメントすると、予期しない結果が発生する可能性があります。

例

次の例では、存続時間のデクリメントをイネーブルにして、ICMP 到達不能レート制限を設定します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
icmp unreachable	ICMP 到達不能メッセージが ASA を通過可能なレートを制御します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
show service-policy	サービス ポリシー設定を表示します。

set connection timeout

ポリシー マップ内のトラフィック クラスに対して接続タイムアウトを指定するには、クラス コンフィギュレーション モードで **set connection timeout** コマンドを使用します。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

no set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

構文の説明

dcd [*retry_interval* [*max_retries*]]	デッド接続検出（DCD）をイネーブルにします。DCD では、デッド接続を検出して、トラフィックをまだ処理できる接続を期限切れにすることなく、そのデッド接続を期限切れにすることができます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。TCP 接続がタイムアウトすると、ASA は、エンドホストに DCD プローブを送信して接続の有効性を判断します。最大再試行回数を超えてもエンドホストの一方が応答しない場合、ASA はその接続を解放します。両方のエンドホストが応答して接続の有効性が確認されると、ASA はアクティビティ タイムアウトを現在時刻に更新し、それに応じてアイドル タイムアウトを再スケジュールします。 トランスペアレント ファイアウォール モードで動作している場合、エンドポイントにスタティック ルートを設定する必要があります。バージョン 9.13(1) 以前では、クラスタ内で DCD を使用できません。 次のオプション値を設定できます。 • *retry_interval*：DCD プローブに応答がない場合に次のプローブを送信するまでの *hh*:*mm*:*ss* 形式の間隔を 0:0:1 ～ 24:0:0 の範囲で指定します。デフォルト値は 0:0:15 です。 クラスタまたは高可用性構成で動作しているシステムでは、間隔を 1 分（0:1:0）未満に設定しないことを推奨します。接続をシステム間で移動する必要がある場合、必要な変更には 30 秒以上かかり、変更が行われる前に接続が削除される場合があります。 • *max_retries*：接続が無活動状態であると宣言するまでに失敗する DCD の連続再試行回数を設定します。最小値は 1、最大値は 255 です。デフォルトは 5 分です。
embryonic *hh*:*mm*:*ss*	TCP 初期（ハーフオープン）接続が閉じられるまでのタイムアウト期間を 0:0:5 ～ 1193:0:0 の範囲で設定します。デフォルト値は 0:0:30 です。値を 0 に設定することもできます。これは、接続がタイムアウトになることはないことを意味します。初期接続とは、スリーウェイ ハンドシェイクが完了していない TCP 接続です。
half-closed *hh*:*mm*:*ss*	ハーフクローズ接続が閉じられるまでのアイドル タイムアウト期間を、9.1(1) 以前の場合は 0:5:0 ～ 1193:0:0 の範囲、9.1(2) 以降の場合は 0:0:30 ～ 1193:0: 0 の範囲で設定します。デフォルト値は 0:10:0 です。値を 0 に設定することもできます。これは、接続がタイムアウトになることはないことを意味します。ハーフクローズの接続は DCD の影響を受けません。また、ASA は、ハーフクローズ接続を切断するときにリセット パケットを送信しません。

idle *hh*:*mm*:*ss*	任意のプロトコルの確立済み接続が閉じられるまでのアイドル タイムアウト期間を設定します。有効な範囲は 0:0:1 ～ 1193:0:0 です。
reset	TCP トラフィックに対してのみ、アイドル接続が削除された後に両方のエンド システムに対して TCP RST パケットを送信します。

デフォルト

timeout コマンドを使用してデフォルトをグローバルに変更していない場合、デフォルトは次のとおりです。

- デフォルトの **embryonic** タイムアウトは 30 秒です。
- デフォルトの **half-closed** アイドル タイムアウトは 10 分です。
- デフォルトの **dcd** *max_retries* の値は 5 です。
- デフォルトの **dcd** *retry_interval* の値は 15 秒です。
- デフォルトの **idle** タイムアウトは 1 時間です。
- デフォルトの **udp** アイドル タイムアウトは 2 分です。
- デフォルトの **icmp** アイドル タイムアウトは 2 秒です。
- デフォルトの **esp** および **ha** アイドル タイムアウトは 30 秒です。
- その他すべてのプロトコルでは、デフォルトのアイドル タイムアウトは 2 分です。
- タイムアウトにならないようにするには、0:0:0 を入力します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	DCD のサポートが追加されました。
8.2(2)	**tcp** キーワードが、すべてのプロトコルのアイドル タイムアウトを制御する **idle** に代わって廃止されました。
9.1(2)	最小 **half-closed** 値が 30 秒(0:0:30)に引き下げられました。
9.13(1)	DCD の設定は、クラスタでサポートされるようになりました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用してこのコマンドを設定します。最初に、**class-map** コマンドを使用して、タイムアウトを適用するトラフィックを定義します。次に、**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラス マップを参照します。クラス コンフィギュレーション モードで、**set connection timeout** コマンドを入力できます。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、CLI 設定ガイドを参照してください。

show service-policy コマンドには、DCD からのアクティビティ量を示すためのカウンタが含まれます。

例

次に、すべてのトラフィックの接続タイムアウトを設定する例を示します。

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# policy-map CONNS
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
ciscoasa(config-pmap-c)# service-policy CONNS interface outside
```

複数のパラメータを使用して **set connection** コマンドを入力するか、各パラメータを別々のコマンドとして入力できます。ASA は、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0
ciscoasa(config-pmap-c)# set connection timeout embryonic 0:40:0
```

この場合、**show running-config policy-map** コマンドの出力には、2 つのコマンドの結果が次の単一の結合コマンドとして表示されます。

```
set connection timeout idle 2:0:0 embryonic 0:40:0
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続の値を設定します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
show service-policy	DCD およびその他のサービス アクティビティのカウンタを表示します。

set default interface

set interface コマンドを **default** オプションとともに使用した場合、一致するトラフィックをルーティングするための最初の試行は、明示ルートをルックアップすることで、通常のルートルックアップを介して実行されなければなりません。通常のルートルックアップに失敗した場合のみ、PBR が指定されたインターフェイスを使用してトラフィックを転送します。その後、「デフォルト」でトリガーされたルックアップと、インターフェイス オプションでトリガーされたルックアップはどちらも、宛先への明示ルートの存在に依存します。「デフォルト」ルックアップは常に成功します。「デフォルト」ルックアップが失敗した場合は、宛先への明示ルートがないことを意味しています。そのため、インターフェイス アクションは適用できません。「set default interface」が設定されている場合は、「Null0」のみをインターフェイスとして設定できます。このオプションが設定されており、通常のルート ルックアップで宛先への明示ルート（デフォルト以外のルート）が判明しない場合、トラフィックはドロップされます。

set default interface Null0

no set default interface Null0

構文の説明

interface	パケットの転送先インターフェイス。

デフォルト

このコマンドにはデフォルトはありません。set 処理として、Null0 インターフェイスが指定されている必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、特定のユーザに異なるデフォルト ルートを提供します。Cisco ASA が宛先への明示ルートを持たない場合、パケットはこのインターフェイスにルーティングされます。set default interface コマンドでアップとして指定された最初のインターフェイスが使用されます。オプションで指定されたインターフェイスは、次に試行されます。

ポリシー ルーティング パケットに関する条件を定義するには、**ip policy route-map** インターフェイス コンフィギュレーション コマンド、**route-map** グローバル コンフィギュレーション コマンド、match および set route-map コンフィギュレーション コマンドを使用します。**ip policy route-map** コマンドは、名前でルート マップを識別します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。**match** コマンドは、一致基準（ポリシー ルーティングが発生する条件）を指定します。**set** コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

IPv6 対応の PBR で、ポリシー ルーティング パケットに関する条件を定義するには、match および set route-map コンフィギュレーション コマンドとともに、**ipv6 policy route-map** または **ipv6 local policy route-map** コマンドを使用します。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. set ip next-hop
2. set interface
3. set ip default next-hop
4. set default interface

例

```
(config)# route-map testmap
(config-route-map)# set default interface Null0
(config)# show run route-map
!
route-map testmap permit 10
  set default interface Null0
!
(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                default interface Null0
```

set dscp

set dscp コマンドは、一致する IP パケットの QoS ビットを設定するために使用されます。

set ip dscp {0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef }

no set ip dscp

set ipv6 dscp {0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef }

no set ipv6 dscp

構文の説明

0 ～ 63	DSCP 値の数値範囲。
af	相対的優先転送クラス
ef	緊急転送
デフォルト	
cs	

デフォルト

ToS バイトの DSCP 値は設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

DSCP ビットを設定すると、他の Quality of Service（QoS）機能がビット設定で動作するようになります。

相互に排他的な DSCP と precedence

set dscp コマンドを set precedence コマンドとともに使用して同じパケットをマークすることはできません。2 つの値（DSCP および precedence）は相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

precedence の値とキューイング

マーキングされたトラフィックには、ネットワークによってプライオリティ（または緊急処理のタイプ）が設定されます。通常は、ネットワーク エッジ（または管理ドメイン）で Precedence 値を設定します。データは、precedence に従ってキューイングされます。重み付け均等化キューイング（WFQ）で、輻輳ポイントでの優先順位の高いトラフィックの処理を高速化できます。Weighted Random Early Detection（WRED; 重み付けランダム早期検出）により、輻輳時の優先順位の高いトラフィックの損失率を他のトラフィックより確実に小さくできます。

「from-field」パケットマーキング カテゴリの使用

このコマンドを、拡張パケット マーキング機能の一部として使用すると、DSCP 値のマッピングと設定に使用される「from-field」パケットマーキング カテゴリを指定できます。「from-field」パケットマーキング カテゴリは次のとおりです。

- サービス クラス（CoS）
- QoS group

「from-field」カテゴリを指定したが、table キーワードと適用可能な table-map-name 引数を指定していない場合、デフォルト アクションは、「from-field」カテゴリに関連付けられた値を DSCP 値としてコピーすることです。たとえば、set dscp cos コマンドを設定する場合、CoS 値がコピーされ、DSCP 値として使用されます。

（注） CoS フィールドは 3 ビット フィールドで、DSCP フィールドは 6 ビット フィールドです。set dscp cos コマンドを設定する場合、CoS フィールドの 3 ビットのみが使用されます。

set dscp qos-group コマンドを設定する場合、QoS グループ値がコピーされ、DSCP 値として使用されます。

DSCP の有効値の範囲は 0 ～ 63 の数字です。QoS グループの有効値の範囲は 0 ～ 99 です。したがって、set dscp qos-group コマンドを設定する場合、次の点に注意してください。

- QoS グループの値が両方の値の範囲（たとえば、44）にある場合、packet-marking 値がコピーされ、パケットがマーク付けされます。
- QoS グループの値が DSCP の範囲を超える場合（たとえば、77）、packet-marking 値はコピーされず、パケットはマーク付けされません。アクションは実行されません。

IPv6 環境での DSCP 値の設定

このコマンドを IPv6 環境で使用すると、デフォルトで IP パケットと IPv6 パケットの両方が照合されます。ただし、この機能によって設定される実際のパケットは、この機能を含むクラスマップの一致基準に合致するパケットのみです。

IPv6 パケットのみに対する DSCP 値の設定

IPv6 値のみの DSCP 値を設定するには、match protocol ipv6 コマンドを使用する必要があります。このコマンドがない場合、precedence 一致では、デフォルトで、IPv4 パケットと IPv6 パケットの両方で一致が発生します。

IPv4 パケットのみに対する DSCP 値の設定

IPv4 値のみの DSCP 値を設定するには、適切な match ip コマンドを使用する必要があります。このコマンドを使用しないと、他の一致基準に応じて、クラス マップが IPv6 パケットと IPv4 パケットの両方に合致し、DSCP 値が両方のタイプのパケットで機能することがあります。

例

```
(config)# route-map testmapv4
(config-route-map)# set ip dscp af22
(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip dscp af22
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
                ip dscp af22
(config)# route-map testmapv6
(config-route-map)# set ipv6 dscp cs6
(config)# show run route-map
!
route-map testmapv6 permit 10
  set ipv6 dscp cs6
!
(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                ipv6 dscp cs6
```

set ikev1 transform-set

IPsec プロファイルに IPsec IKEv1 プロポーザルを指定するには、IPsec プロファイル コンフィギュレーション モードで **set ikev1 transform-set** コマンドを使用します。IPsec IKEv1 プロポーザルを削除するには、このコマンドの **no** 形式を使用します。

set ikev1 transform-set *transform-set name*

no set ikev1 transform-set *transform-set name*

構文の説明

transform-set name	IPsec IKEv1 プロポーザルの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPsec プロファイル設定	• あり	• なし	• あり	• なし	• -

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、IPsec プロファイルに IKEv1 プロポーザルを指定する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set ikev1 transform-set
```

関連コマンド

コマンド	説明
crypto ipsec profile	新しい IPsec プロファイルを作成します。
responder-only	VTI トンネル インターフェイスをレスポンダ専用モードに設定します。
set pfs	PFS グループを IPsec プロファイル設定に使用するように指定します。
set security-association lifetime	IPsec プロファイル設定でのセキュリティ アソシエーションの期間を指定します。これは、キロバイト単位か秒単位、またはその両方で指定します。
set trustpoint	VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

set interface

set interface コマンドは、一致するトラフィックを転送する際に経由する必要があるインターフェイスを設定するために使用されます。パケットの転送先として有効な稼働中のインターフェイスが見つかるまで、指定された順序でインターフェイスが評価される場合は、複数のインターフェイスを設定できます。インターフェイス名を Null0 として指定すると、ルート マップに一致するトラフィックはすべてドロップされます。

set interface [...*interface***]**

no set interface [...*interface***]**

構文の説明

interface	パケットの転送先インターフェイス。

デフォルト

コマンドのデフォルト値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ポリシー ルーティング パケットに関する条件を定義するには、**ip policy route-map** インターフェイス コンフィギュレーション コマンド、route-map グローバル コンフィギュレーション コマンド、match および set route-map コンフィギュレーション コマンドを使用します。**ip policy route-map** コマンドは、名前でルート マップを識別します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準（ポリシー ルーティングが発生する条件）を指定します。set コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

IPv6 対応の PBR で、ポリシー ルーティング パケットに関する条件を定義するには、match および **set route-map** コンフィギュレーション コマンドとともに、**ipv6 policy route-map** または **ipv6 local policy route-map** コマンドを使用します。

set interface コマンドで指定された最初のインターフェイスがダウン状態になると、オプションで指定されたインターフェイスが順番に試行されます。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. set ip next-hop
2. set interface
3. set ip default next-hop
4. set default interface

有用なネクスト ホップはインターフェイスで暗黙指定されます。ネクスト ホップとインターフェイスが見つかるとすぐに、そのパケットがルーティングされます。

例

```
ciscoasa(config)# route-map testmap
ciscoasa(config-route-map)# set interface outside
ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  set interface outside
!
ciscoasa(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                interface outside
```

set ip df

set ip df コマンドは、一致する IP パケットに df（do-not-fragment）ビットを設定するために使用されます。

set ip df [0|1]

no set ip df

構文の説明

0	df ビットを 0 に設定（df ビットをクリア）して、パケット フラグメンテーションを許可します。
1	df ビットを 1 に設定して、パケット フラグメンテーションを禁止します。

デフォルト

このコマンドにはデフォルトはありません。set 処理で、0 または 1 のいずれかを df ビットとして指定する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

パス MTU 検出（PMTUD）を使用して、フラグメンテーションを回避する IP パケットの MTU 値を決定できます。ICMP メッセージがルータによってブロックされると、パス MTU は破棄され、df ビットが設定されたパケットは廃棄されます。set ip df コマンドを使用して df ビットをクリアし、パケットのフラグメンテーションと送信を許可します。フラグメンテーションによって、ネットワーク上のパケット転送速度が低下する場合がありますが、アクセス リストを使用して、df ビットがクリアされるパケット数を制限できます。

（注） df ビットが設定されている場合、一部の IP トランスミッタ（特に Linux のいくつかのバージョン）が、IP ヘッダーの ID フィールド（IPid）をゼロに設定することがあります。ルータがこのようなパケットの df ビットをクリアする場合やそのパケットがその後フラグメント化される場合には、IP レシーバは、おそらく元の IP パケットに正常にリアセンブルすることができません。

例

```
(config)# route-map testmap
(config-route-map)# set ip df 1
(config)# show run route-map
!
route-map testmap permit 10
  set ip df 1
!
(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                ip df 1
```

set ip default next-hop

set ip next-hop コマンドを **default** オプションとともに使用した場合、一致するトラフィックをルーティングするための最初の試行は、明示ルートをルックアップすることで、通常のルートルックアップを介して実行されなければなりません。通常のルートルックアップが失敗した場合のみ、ポリシー ベース ルーティング（PBR）は、指定されたネクスト ホップ IP アドレスを使用してトラフィックを転送します。

set ip default next-hop *ip-address* [*... ip-address*]

no set ip default next-hop *ip-address* [*... ip-address*]

set default ipv6next-hop *ip-address* [**...** *ip-address*]

no set default ipv6 next-hop *ip-address* [**...** *ip-address*]

構文の説明

ip-address	パケットが出力される出力先ネクスト ホップの IP アドレス。隣接ルータである必要はありません。
ipv6-address	パケットが出力されるネクスト ホップの IPv6 アドレス。隣接ルータである必要はありません。

デフォルト

このコマンドはデフォルトでは無効になっています。set 処理には、1 つ以上のネクストホップ IP アドレスを指定する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、特定のユーザに異なるデフォルト ルートを提供します。ソフトウェアがパケットの宛先への明示ルートを持たない場合、パケットは次のネクスト ホップにルーティングされます。**set ip default next-hop** コマンドで指定された最初のネクスト ホップはルータに隣接している必要があります。次に、オプションの IP アドレスが使用されます。

ポリシー ルーティング パケットに関する条件を定義するには、ip policy route-map インターフェイス コンフィギュレーション コマンド、route-map グローバル コンフィギュレーション コマンド、match および set route-map コンフィギュレーション コマンドを使用します。ip policy route-map コマンドは、名前でルート マップを識別します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準（ポリシー ルーティングが発生する条件）を指定します。set コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

set next-hop コマンドで指定された最初のネクスト ホップがダウン状態になると、任意で指定された IP アドレスが使用されます。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. **set next-hop**
2. **set interface**
3. **set default next-hop**
4. **set default interface**

（注） set ip next-hop と set ip default next-hop は類似のコマンドですが、操作順が異なります。set ip next-hop コマンドを設定すると、最初にポリシー ルーティングを使用してからルーティング テーブルを使用します。set ip default next-hop コマンドを設定すると、最初にルーティング テーブルを使用してから指定のネクスト ホップをポリシー ルーティングします。

例

```
(config)# route-map testmapv4
(config-route-map)# set ip default next-hop 1.1.1.1
(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip default next-hop 1.1.1.1
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
Match clauses:
Set clauses:
ip default next-hop 1.1.1.1
(config)# route-map testmapv6
(config-route-map)# set ipv6 default next-hop 2001::1
(config)# show run route-map
!
route-map testmapv6 permit 10
  set ipv6 default next-hop 2001::1
!
(config)# show route-map testmapv6
route-map testmapv6, permit, sequence 10
Match clauses:
Set clauses:
ipv6 default next-hop 2001::1
```

set ip next-hop

ポリシー ルーティングにおいてルート マップの match 句を通過するパケットの出力先を示すには、ルートマップ コンフィギュレーション モードで **set ip next-hop** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

set ip next-hop *ip-address* [*... ip-address*] [**peer-address**]

no set ip next-hop *ip-address* [**...** *ip-address*] [**peer-address**]

set ipv6 next-hop

構文の説明

ip-address	パケットが出力される出力先ネクスト ホップの IP アドレス。隣接ルータである必要はありません。
peer-address	（オプション）ネクスト ホップを BGP ピア アドレスに設定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

コマンド構文の省略記号（...）は、コマンド入力で *ip-address* 引数に複数の値を含めることができることを示します。

ポリシー ルーティング パケットに関する条件を定義するには、**ip policy route-map** インターフェイス コンフィギュレーション コマンド、**route-map** グローバル コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用します。**ip policy route-map** コマンドは、名前でルート マップを識別します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、*一致基準*（ポリシー ルーティングが発生する条件）を指定します。**set** コマンドは、*set 処理*（**match** コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

set next-hop コマンドで指定された最初のネクスト ホップがダウン状態になると、任意で指定された IP アドレスが使用されます。

BGP ピアのインバウンド ルート マップで **peer-address** キーワードを指定し、**set next-hop command** コマンドを使用すると、受信した一致するルートのネクスト ホップをネイバー ピア アドレスに設定し、サードパーティのネクスト ホップを上書きします。したがって、同じルート マップを複数の BGP ピアに適用すると、サードパーティのネクストホップを上書きできます。

BGP ピアのアウトバウンド ルート マップで **peer-address** キーワードを指定し、**set next-hop** コマンドを使用すると、アドバタイズされた一致するルートのネクスト ホップをローカル ルータのピア アドレスに設定し、ネクスト ホップ計算をディセーブルにします。他のルートではなく、一部のルートにネクスト ホップを設定できるので、**set next-hop** コマンドは、（ネイバー単位の）**neighbor next-hop-self** コマンドよりも詳細に設定できます。**neighbor next-hop-self** コマンドは、そのネイバーに送信されたすべてのルートにネクスト ホップを設定します。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. **set next-hop**
2. **set interface**
3. **set default next-hop**
4. **set default interface**

（注） 反映されたルートの一般的な設定エラーを回避するために、BGP ルート リフレクタ クライアントに適用するルート マップで **set next-hop** コマンドを使用しないでください。

例

次の例では、3 台のルータが同じ LAN 上にあります（IP アドレス 10.1.1.1, 10.1.1.2 および 10.1.1.3）。それぞれが異なる自律システム（AS）です。**set ip next-hop peer-address** コマンドは、ルート マップと一致する、リモート自律システム 100 内のルータ（10.1.1.3）からリモート自律システム 300 内のルータ（10.1.1.1）へのトラフィックが、LAN への相互接続上で自律システム 100 内のルータ（10.1.1.1）に直接送信されるのではなく、ルータ bgp 200 を通過するように指定します。

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.1.1.3 remote-as 300
ciscoasa(config-router-af)# neighbor 10.1.1.3 route-map set-peer-address out
ciscoasa(config-router-af)# neighbor 10.1.1.1 remote-as 100
ciscoasa(config-route-af)# route-map set-peer-address permit 10
ciscoasa(config-route-map)# set ip next-hop peer-address
```

set ip next-hop recursive

set ip next-hop と **set ip default next-hop** はどちらも、ネクストホップが直接接続されたサブネット上に存在している必要があります。**set ip next-hop recursive** では、ネクストホップ アドレスが直接接続されている必要はありません。代わりにネクストホップ アドレスで再帰ルックアップが実行され、一致するトラフィックは、ルータで使用されているルーティング パスに従って、そのルート エントリで使用されているネクストホップに転送されます。

ネクストホップの再帰ルックアップは、IPv6 に対して、またはデフォルト キーワードが指定されている場合には、適用できません。

set ip next-hop recursive [*ipv4-address*]

no set ip next-hop recursive [*ipv4-address*]

構文の説明

ipv4-address	パケットが出力される出力先ネクスト ホップの IP アドレス。隣接ルータである必要はありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ポリシー ルーティング パケットに関する条件を定義するには、**ip policy route-map** インターフェイス コンフィギュレーション コマンド、route-map グローバル コンフィギュレーション コマンド、match および set route-map コンフィギュレーション コマンドを使用します。ip policy route-map コマンドは、名前でルート マップを識別します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準（ポリシー ルーティングが発生する条件）を指定します。set コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

set ip next-hop コマンドで指定された最初のネクスト ホップに関連付けられたインターフェイスがダウン状態になると、オプションで指定された IP アドレスが順番に試行されます。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. set ip next-hop
2. set interface
3. set ip default next-hop
4. set default interface

(注) **set ip next-hop** と **set ip default next-hop** は類似のコマンドですが、操作順が異なります。set ip next-hop コマンドを設定すると、最初にポリシー ルーティングを使用してからルーティング テーブルを使用します。set ip default next-hop コマンドを設定すると、最初にルーティング テーブルを使用してから指定のネクスト ホップをポリシー ルーティングします。

例

```
(config)# route-map testmapv4
(config-route-map)# set ip next-hop recursive 1.1.1.1
(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip next-hop recursive 1.1.1.1
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
                ip next-hop recursive 1.1.1.1
```

set ip next-hop verify-availability

set ip next-hop verify-availability は、ネクストホップの到達可能性を確認するために、SLA モニタ トラッキング オブジェクトとともに設定できます。複数のネクストホップの可用性を確認するために、複数の **set ip next-hop verify-availability** コマンドを異なるシーケンス番号と異なるトラッキング オブジェクトで設定できます。

set ip next-hop verify-availability [*sequence number*] **track** [*tracked-object-number*]

no set ip next-hop verify-availability [*sequence number*] **track** [*tracked-object-number*]

構文の説明

sequence-number	ネクスト ホップのシーケンス。指定できる範囲は 1 ～ 65535 です。
track	トラッキング方式はトラックです。
tracked-object-number	トラッキング サブシステムが追跡しているオブジェクト数。指定できる範囲は 1 ～ 500 です。

デフォルト

コマンドのデフォルト値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

set ip next-hop verify-availability コマンドは、次の 2 とおりの方法で使用できます。

- ネクスト ホップの到達可能性を確認するための Cisco Discovery Protocol（CDP）を使用したポリシーベース ルーティング（PBR）。
- リモート デバイスが到達可能であるかどうか確認するために Internet Control Message Protocol（ICMP）ping または HTTP GET リクエストを使用してオブジェクト トラッキングをサポートするオプションの引数。

CDP 検証の使用方法

このコマンドは、ルータがポリシー ルーティングを試みる前に、ネクスト ホップが到達可能であることを確認するために使用されます。このコマンドには次のような特長があります。

- パフォーマンスが若干低下します。
- CDP がインターフェイスに設定されている必要があります。
- ネクスト ホップは、CDP が有効なシスコ デバイスである必要があります。
- プロセス スイッチングと Cisco Express Forwarding（CEF）ポリシー ルーティングでサポートされていますが、CDP ネイバー データベースの依存関係のため、分散型 CEF（dCEF）では利用できません。

ルータがパケットをネクスト ホップにポリシー ルーティングしていて、ネクスト ホップがダウンしている場合、ルータがネクスト ホップ（ダウン中）に対して Address Resolution Protocol（ARP）を使用しようとして失敗します。この動作はいつまでも続きます。この状況の発生を防ぐには、set ip next-hop verify-availability コマンドを使用して、そのネクスト ホップにルーティングする前に、ルート マップのネクスト ホップが CDP ネイバーであることを確認するようにルータを設定します。

いくつかのメディアまたはカプセル化は CDP をサポートしていない、またはルータにトラフィックを送信しているのがシスコ デバイスではない場合があるため、このコマンドはオプションです。

このコマンドが設定され、ネクスト ホップが CDP ネイバーではない場合、ルータは次のネクスト ホップ（存在する場合）を検索します。ネクスト ホップがない場合は、パケットはポリシー ルーティングされません。

このコマンドが設定されていない場合、パケットは正常にポリシー ルーティングされるか、または永続的にルーティングされないままになります。

いくつかのネクストホップのみの可用性を選択的に確認する場合、異なる基準（アクセス リストの照合またはパケット サイズの照合を使用）で異なるルート マップ エントリ（同じルート マップ名）を設定してから、選択的に set ip next-hop verify-availability コマンドを使用することもできます。

オブジェクト トラッキングの使用方法

オブジェクト トラッキングをサポートするオプションの引数とともに、このコマンドを使用すると、PBR は次の基準に基づいて決定を下すことができます。

- リモート デバイスへの ICMP ping の到達可能性。
- リモート デバイスで稼働中のアプリケーション（たとえば、デバイスが HTTP GET リクエストに応答する）。
- ルーティング情報ベース（RIB）に存在するルート（たとえば、10.2.2.0/24 が RIB に存在する場合のみ、ポリシー ルーティングする）。
- インターフェイスの状態（たとえば、E0 で受信されたパケットは E2 がダウンしている場合のみ、E1 にポリシー ルーティングする必要がある）。

オブジェクト トラッキングは次のように機能します。PBR は、特定のオブジェクトのトラッキングを対象としていることをトラッキング プロセスに通知します。トラッキング プロセスは、そのオブジェクトの状態が変化したときに、それを PBR に通知します。この通知はレジストリを介して行われ、イベント駆動型です。

トラッキング サブシステムは、オブジェクトの状態をトラッキングする役割を担います。オブジェクトには、トラッキング プロセスによって定期的に ping が実行される IP アドレスを指定できます。オブジェクトの状態（アップまたはダウン）は、トラック レポート データ構造に保存されます。トラッキング プロセスは、トラッキング オブジェクト レポートを作成します。次に、ルート マップを設定している exec プロセスが、所定のオブジェクトが存在するかどうかを判別するために、トラッキング プロセスにクエリできます。オブジェクトが存在する場合、トラッキング サブシステムはトラッキングを開始し、オブジェクトの初期状態を読み取ります。オブジェクトの状態が変化すると、トラッキング プロセスはオブジェクトの状態が変わったことを、このプロセスをトラッキングしているすべてのクライアントに通知します。そのため、PBR が使用しているルート マップ構造は、トラック レポート内のオブジェクトの現在の状態を反映して更新できます。このプロセス間通信は、レジストリと共有トラック レポートを使用して実行されます。

（注） CDP およびオブジェクト トラッキング コマンドを混在させると、トラッキングされているネクスト ホップが最初に試行されます。

例

```
ciscoasa(config)# sla monitor 1
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 1.1.1.1 interface outside
ciscoasa(config)# sla monitor schedule 1 life forever start-time now
ciscoasa(config)# track 1 rtr 1 reachability
ciscoasa(config)#
ciscoasa(config)# route-map testmapv4
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.1 10 track 1
ciscoasa(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip next-hop verify-availability 1.1.1.1 10 track 1
!
ciscoasa(config)# show route-map testmap
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
               ip next-hop verify-availability 1.1.1.1 10 track 1
```

set local-preference

自律システム パスのプリファレンス値を指定するには、ルートマップ コンフィギュレーション モードで set local-preference コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

set local-preference *number-value*

no set local-preference *number-value*

構文の説明

number-value	プリファレンス値。0 ～ 4294967295 の整数。

デフォルト

プリファレンス値は 100 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

プリファレンスは、ローカル自律システム内のすべてのルータにのみ送信されます。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、**route-map** グローバル コンフィギュレーション コマンドと、match および set **route-map** コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準、つまり現在の **route-map** コマンドに再配布が許可される条件を指定します。set コマンドは、set 処理、つまり match コマンドで指定した基準を満たしている場合に実行する特定の再配布アクションを指定します。**no route-map** コマンドは、ルート マップを削除します。

set **route-map** コンフィギュレーション コマンドを使用すると、ルート マップのすべての一致基準が満たされたときに実行される再配布 set 処理を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

bgp default local-preference コマンドを使用して、デフォルトのプリファレンス値を変更できます。

例

次に、アクセス リスト 1 に含まれるすべてのルートに対して、ローカル プリファレンスを 100 に設定する例を示します。

```
ciscoasa(config-route-map)# route-map map-preference
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

set metric

ルート マップ内の OSPF およびその他のダイナミック ルーティング プロトコルのルートのメトリック値を設定するには、ルートマップ コンフィギュレーション モードで **set metric** コマンドを使用します。OSPF およびその他のダイナミック ルーティング プロトコルのメトリック値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

set metric *metric-value* | [***bandwidth delay reliability loading mtu***]

no set metric *metric-value* | [***bandwidth delay reliability loading mtu***]

構文の説明

帯域幅	ルートの EIGRP 帯域幅（kbps）。有効値の範囲は、0 ～ 4294967295 です。
delay	EIGRP ルート遅延（10 マイクロ秒単位）。有効値の範囲は、0 ～ 4294967295 です。
loading	0 ～ 255 の数値で表される、ルートの有効な EIGRP 帯域幅。値 255 は、100 % のロードを意味します。
metric-value	数値で表される、OSPF およびその他のダイナミック ルーティング プロトコル（EIGRP 以外）のルートのメトリック値。有効値の範囲は、0 ～ 4294967295 です。
mtu	EIGRP のルートの最小 MTU サイズ（バイト単位）。有効値の範囲は、0 ～ 4294967295 です。
信頼性	0 ～ 255 の数値で表される、EIGRP のパケット伝送の成功確率。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(5)	ルート マップで EIGRP をサポートするために、*bandwidth*、*delay*、*reliability*、*loading*、および *mtu* 引数が追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

no set metric コマンドを使用すると、OSPF およびその他のダイナミック ルーティング プロトコルのメトリック値をデフォルトに戻すことができます。このコンテキストでは、*metric-value* 引数は 0 ～ 4294967295 の整数です。

例

次に、OSPF ルーティングのルート マップを設定する例を示します。

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
```

次に、ルート マップ内の EIGRP のメトリック値を設定する例を示します。

```
ciscoasa(config)# access-list route-out line 1 standard permit 10.1.1.0 255.255.255.0
ciscoasa(config)# route-map rmap permit 10
ciscoasa(config-route-map)# set metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show route-map rmap
route-map rmap, permit, sequence 10
  Match clauses:
    ip address (access-lists): route-out
  Set clauses:
    metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show running-config route-map
route-map rmap permit 10
 match ip address route-out
 set metric 10000 60 100 1 1500
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。

set metric-type

OSPF メトリック ルートのタイプを指定するには、ルート マップ コンフィギュレーション モードで **set metric-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set metric-type{**type-1** | **type-2**}

no set metric-type

構文の説明

type-1	指定された自律システムの外部にある OSPF メトリック ルートのタイプを指定します。
type-2	指定された自律システムの外部にある OSPF メトリック ルートのタイプを指定します。

デフォルト

デフォルトは、**type-2** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、OSPF ルーティングのルート マップを設定する例を示します。

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# set metric-type type-2
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
ciscoasa(config-route-map)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

set metric-type internal

ネクスト ホップの内部ゲートウェイ プロトコル（IGP）のメトリックと照合するために外部 BGP（eBGP）ネイバーにアドバタイズされたプレフィックスに Multi Exit Discriminator（MED）を設定するには、ルートマップ コンフィギュレーション モードで **set metric-type internal** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

set metric-type internal

no set metric-type internal

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを指定すると、BGP はルートのネクスト ホップと関連付けられた IGP メトリックに対応する MED 値をアドバタイズします。このコマンドは、生成された内部 BGP（iBGP）生成ルートおよび eBGP 生成ルートに適用されます。

このコマンドを使用すると、共通の自律システム内の複数の BGP スピーカーが 1 つの特定のプレフィックスに対して異なる MED 値をアドバタイズできます。また、IGP メトリックが変更された場合、BGP によって 10 分ごとにルートが再アドバタイズされることに注意してください。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、**route-map** グローバル コンフィギュレーション コマンドと、**match** および **set** route-map コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、*一致基準*（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、*set 処理*（**match** コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドは、ルート マップを削除します。

set route-map コンフィギュレーション コマンドは、ルート マップのすべての一致基準が満たされたときに実行される再配布 *set 処理*を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

(注) このコマンドは、ボーダー ゲートウェイ プロトコル（BGP）へのルートの再配布ではサポートされていません。

例

次に、ネイバー 172.16.2.3 へのすべてのアドバタイズ済みルートの MED 値を、ネクスト ホップの対応する IGP メトリックに設定する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 172.16.0.0
ciscoasa(config-router-af)# neighbor 172.16.2.3 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.2.3 route-map setMED out
ciscoasa(config-route-map)# route-map setMED permit 10
ciscoasa(config-route-map)# match as-path as-path-acl
ciscoasa(config-route-map)# set metric-type internal
ciscoasa(config-route-map)# ip as-path access-list as-path-acl permit .*
```

set origin

BGP 送信元コードを設定するには、ルートマップ コンフィギュレーション モードで **set origin** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

set origin {**igp** | **egp** *autonomous-system-number* | **incomplete**}

no set origin {**igp** | **egp** *autonomous-system-number* | **incomplete**}

構文の説明

autonomous-system-number	リモート自律システム番号。この引数の値の範囲は、1 ～ 65535 の有効な自律システム番号です。
egp	外部ゲートウェイ プロトコル(EGP)のローカル システム。
igp	内部ゲートウェイ プロトコル(IGP)のリモート システム。
incomplete	不明な継承。

デフォルト

ルートの起点は、メイン IP ルーティング テーブルのルートのパス情報に基づいています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ルートの起点を設定する場合は、match 句を使用する必要があります(「permit everything」リストを指している場合でも)。ルートを BGP に再配布するときの特定の起点を設定するには、このコマンドを使用します。ルートが再配布されると、通常、起点は incomplete として記録され、BGP テーブルでは ? で示されます。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、**route-map** グローバル コンフィギュレーション コマンドと、**match** および **set** route-map コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、*一致基準*(現在の **route-map** コマンドで再配布が許可される条件)を指定します。**set** コマンドは、*set 処理*(**match** コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクション)を指定します。**no route-map** コマンドは、ルート マップを削除します。

set route-map コンフィギュレーション コマンドは、ルート マップのすべての一致基準が満たされたときに実行される再配布 *set 処理*を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

例

次に、ルート マップを IGP に送信するルートの発信を設定する例を示します。

```
ciscoasa(config-route-map)# route-map set_origin
ciscoasa(config-route-map)# match as-path 10
ciscoasa(config-route-map)# set origin igp
```

set pfs

IPsec プロファイルに PFS グループを指定するには、IPsec プロファイル コンフィギュレーション モードで **set pfs** コマンドを使用します。PFS グループを削除するには、このコマンドの **no** 形式を使用します。

set pfs *Diffie-Hellman group* [**group14**]

no set pfs *Diffie-Hellman group* [**group14**]

構文の説明

Diffie-Hellman グループ	*Diffie-Hellman group (dh group)* の名前を指定します。
group14	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPsec プロファイル設定	• あり	• なし	• あり	• なし	• -

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。
9.13(1)	グループ 14 のサポートが追加されました。**group2** および **group5** コマンド オプションは廃止され、以降のリリースで削除されます。

例

次に、group14 を pfs として設定する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set pfs group14
```

関連コマンド

コマンド	説明
crypto ipsec profile	新しい IPsec プロファイルを作成します。
responder-only	VTI トンネル インターフェイスをレスポンダ専用モードに設定します。
set ikev1 transform-set	IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。

コマンド	説明
set security-association lifetime	IPsec プロファイル設定でのセキュリティ アソシエーションの期間を指定します。これは、キロバイト単位か秒単位、またはその両方で指定します。
set trustpoint	VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

set security-association lifetime

IPsec プロファイル設定でセキュリティ アソシエーションの期間を指定するには、IPsec プロファイル コンフィギュレーション モードで **set security-association lifetime** コマンドを使用します。これは、キロバイト単位か秒単位、またはその両方で指定します。セキュリティ アソシエーションのライフタイム設定を削除するには、このコマンドの **no** 形式を使用します。

set security-association lifetime {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

no set security-association lifetime {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

構文の説明

kilobytes {*number* | **unlimited**}	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。指定できる範囲は 10 ～ 2147483647 KB です。グローバル デフォルトは 4,608,000 キロバイトです。 この設定は、リモート アクセス VPN 接続には適用されません。サイト間 VPN のみに適用されます。
seconds *number*	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。指定できる範囲は 120 ～ 214783647 秒です。グローバルのデフォルトは 28,800 秒（8 時間）です。 この設定は、リモート アクセスとサイト間 VPN の両方に適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPsec プロファイル設定	• あり	• なし	• あり	• なし	• -

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

クリプト マップのセキュリティ アソシエーションは、グローバル ライフタイムに基づいてネゴシエートされます。

IPsec セキュリティ アソシエーションでは、共有秘密キーが使用されます。これらのキーとセキュリティ アソシエーションは、両方同時にタイムアウトになります。

特定のクリプト マップ エントリでライフタイム値が設定されている場合、ASA は、セキュリティ アソシエーションのネゴシエート時に新しいセキュリティ アソシエーションを要求するときに、ピアへの要求でクリプト マップ ライフタイム値を指定し、これらの値を新しいセキュリティ アソシエーションのライフタイムとして使用します。ASA は、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します

サイト間 VPN 接続の場合、「時間指定」と「トラフィック量」の 2 つのライフタイムがあります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。リモート アクセス VPN セッションでは、指定時刻ライフタイムのみが適用されます。

(注) ASA では、クリプト マップ、ダイナミック マップ、および IPsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみが ASA によって停止させられます。たとえば、アクセス リスト内のエントリを削除して、クリプト マップに関連付けられた既存のアクセス リストを変更した場合、関連する接続だけがダウンします。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

例

次に、セキュリティ アソシエーションの有効期間の値を設定する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set security-association lifetime seconds 120 kilobytes
10000
```

関連コマンド

コマンド	説明
crypto ipsec profile	新しい IPsec プロファイルを作成します。
responder-only	VTI トンネル インターフェイスをレスポンダ専用モードに設定します。
set ikev1 transform-set	IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。
set pfs	PFS グループを IPsec プロファイル設定に使用するように指定します。
set trustpoint	VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

set trustpoint

VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定するには、IPsec プロファイル コンフィギュレーション モードで **set trustpoint** コマンドを使用します。トラストポイントの設定を削除するには、このコマンドの **no** 形式を使用します。

set trustpoint *name* **chain**

no set trustpoint *name* **chain**

構文の説明

name	トラストポイントの名前を指定します。
chain	証明書チェーンの送信を有効にします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPsec プロファイル設定	• あり	• なし	• あり	• なし	• -

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。

例

次に、セキュリティ アソシエーションの有効期間の値を設定する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set trustpoint TPVTI chain
```

関連コマンド

コマンド	説明
crypto ipsec profile	新しい IPsec プロファイルを作成します。
responder-only	VTI トンネル インターフェイスをレスポンダ専用モードに設定します。
set ikev1 transform-set	IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。
set pfs	PFS グループを IPsec プロファイル設定に使用するように指定します。

setup

対話形式のプロンプトを使用して ASA の最小限度のコンフィギュレーションを設定するには、グローバル コンフィギュレーション モードで **setup** コマンドを入力します。

セットアップ

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	ASA 5510 以降のルーテッド モードでは、設定されたインターフェイスは、「inside」インターフェイスではなく管理*スロット/ポート*インターフェイスになりました。ASA 5505 の場合、設定されたインターフェイスは「inside」インターフェイスではなく VLAN 1 インターフェイスです。
9.0(1)	デフォルト コンフィギュレーション プロンプトが変更され、セットアップ プロセスを終了するための Ctrl + Z がイネーブルになりました。

使用上のガイドライン

フラッシュ メモリにスタートアップ コンフィギュレーションがない場合は、起動時にセットアップ プロンプトが自動的に表示されます。

setup コマンドによって、ASDM 接続を確立するための最小コンフィギュレーションが順を追って示されます。このコマンドは、コンフィギュレーションがないか、コンフィギュレーションが部分的にしかないユニット向けに設計されたものです。工場出荷時のコンフィギュレーションをサポートするモデルを使用している場合は、**setup** コマンドではなく工場出荷時のコンフィギュレーションを使用することを推奨します(デフォルトのコンフィギュレーションに戻すには、**configure factory-default** コマンドを使用します)。

setup コマンドには、「management」という名前が付けられたインターフェイスが必要です。

setup コマンドを入力すると、表 1-1 の情報の入力を求められます。表示されたパラメータにコンフィギュレーションがすでに存在する場合は、そのコンフィギュレーションが角カッコで囲まれて表示されるため、その値をデフォルトとして受け入れるか、または新しい値を入力してその値を上書きできます。使用可能なプロンプトは、モデルによって異なる場合があります。システムの **setup** コマンドには、これらのプロンプトのサブセットが含まれています。

表 1-1　設定プロンプト

プロンプト	説明
`Pre-configure Firewall now through interactive prompts [yes]?`	**yes** または **no** を入力します。**yes** と入力すると、セットアップが続行されます。**no** を入力すると、セットアップが停止し、グローバル コンフィギュレーション プロンプト（ciscoasa(config)#）が表示されます。
`Firewall Mode [Routed]:`	**routed** または **transparent** を入力します。
`Enable password:`	イネーブル パスワードを入力します（パスワードは、3 文字以上である必要があります）。
`Allow password recovery [yes]?`	**yes** または **no** を入力します。
`Clock (UTC):`	このフィールドには何も入力できません。UTC 時間がデフォルトで使用されます。
`Year:`	4 桁の年（2005 など）を入力します。年の範囲は 1993 ～ 2035 です。
`Month:`	月名の先頭の 3 文字（9 月の場合は **Sep** など）を使用して月を入力します。
`Day:`	日付（1 ～ 31）を入力します。
`Time:`	時間、分、および秒を 24 時間形式で入力します。たとえば、午後 8 時 54 分 44 秒の場合は、**20:54:44** と入力します。
`Host name:`	コマンドライン プロンプトに表示するホスト名を入力します。
`Domain name:`	ASA を稼働するネットワークのドメイン名を入力します。
`IP address of host running Device Manager:`	ASDM にアクセスする必要があるホストの IP アドレスを入力します。
`Use this configuration and save to flash (yes)?`	**yes** または **no** を入力します。**yes** を入力すると、内部インターフェイスがイネーブルになり、要求されたコンフィギュレーションがフラッシュ パーティションに書き込まれます。 **no** を入力すると、セットアップ プロンプトが、最初の質問から繰り返されます。 `Pre-configure Firewall now through interactive prompts [yes]?` セットアップを終了する場合は **Ctrl + Z** を入力し、プロンプトを繰り返す場合は **yes** を入力します。

例

次に、**setup** コマンドを完了する例を示します。

```
ciscoasa(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
```

```
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

関連コマンド

コマンド	説明
configure factory-default	デフォルトのコンフィギュレーションに戻します。

set weight

ルーティング テーブルの BGP 重みを指定するには、ルートマップ コンフィギュレーション モードで **set weight** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

set weight *number*

no set weight *number*

構文の説明

number	重み値。0 ～ 65535 の範囲の整数に設定できます。

デフォルト

重みは指定のルート マップによって変更されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

実行された重みは、最初に一致した自律システム（AS）パスに基づいています。自律システム パスが一致したときに表示された重みは、グローバルな **neighbor** コマンドによって割り当てられた重みを上書きします。つまり、**set weight** route-map コンフィギュレーション コマンドで割り当てられた重みは、**neighbor weight** コマンドを使用して割り当てられた重みを上書きします。

例

次に、自律システム パス アクセス リストと一致するルートの BGP 重みを 200 に設定する例を示します。

```
ciscoasa(config-route-map)# route-map set-weight
ciscoasa(config-route-map)# match as-path as_path_acl
iscoasa(config-route-map)# set weight 200
```

sfr

トラフィックを ASA FirePOWER モジュールにリダイレクトするには、クラス コンフィギュレーション モードで **sfr** コマンドを使用します。リダイレクトを削除するには、このコマンドの **no** 形式を使用します。

sfr {**fail-close** | **fail-open**} [**monitor-only**]

no sfr {**fail-close** | **fail-open**} [**monitor-only**]

構文の説明

fail-close	モジュールが使用できない場合にトラフィックをブロックするように ASA を設定します。
fail-open	モジュールが使用できない場合に、ASA ポリシーのみを適用してトラフィックの通過を許可するように ASA を設定します。
monitor-only	トラフィックの読み取り専用コピーをモジュールに送信します(パッシブ モード)。キーワードを指定しない場合、トラフィックはインライン モードで送信されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

クラス コンフィギュレーション モードにアクセスするには、policy-map コマンドを入力します。

ASA に **sfr** コマンドを設定する前または後に、Firepower Management Centerを使用してモジュールにセキュリティ ポリシーを設定します。

sfr コマンドを設定するには、まず、**class-map** コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

トラフィック フロー

ASA FirePOWER モジュールは、ASA から個別のアプリケーションを実行します。ただし、そのアプリケーションは ASA のトラフィック フローに統合されます。ASA でトラフィックのクラスに対して **sfr** コマンドを適用すると、次のように、トラフィックは ASA およびモジュールを経由します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. バックプレーンを介して ASA FirePOWER モジュールにトラフィックが送信されます。
5. モジュールはそのセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. インライン モードでは、有効なトラフィックがバックプレーンを介して ASA に返送されます。ASA FirePOWER モジュールがセキュリティ ポリシーに従ってトラフィックをブロックすることがあり、そのトラフィックは渡されません。パッシブ モードではトラフィックが戻されず、モジュールはトラフィックをブロックできません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

ASA の機能との互換性

ASA には、HTTP インスペクションを含む、多数の高度なアプリケーション インスペクション機能があります。ただし、ASA FirePOWER モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングおよび制御機能です。

ASA FirePOWER モジュールの機能を最大限に活用するには、ASA FirePOWER モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。ASA FirePOWER インスペクションと Cloud Web Security のインスペクションの両方を同じトラフィックに設定すると、ASA では ASA FirePOWER インスペクションのみが実行されます。
- ASA 上の他のアプリケーション インスペクションは ASA FirePOWER モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA FirePOWER モジュールとの間に互換性がありません。
- フェールオーバーをイネーブルにしている場合、ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールがその時点からトラフィックのインスペクションを開始します。古いインスペクションの状態は転送されません。

モニタ専用モード

モニタ専用モードのトラフィック フローは、インライン モードのトラフィック フローと同じです。ただし、ASA FirePOWER モジュールではトラフィックを ASA に戻さない点のみが異なります。代わりに、モジュールはトラフィックにセキュリティ ポリシーを適用し、インライン モードで動作していたらどのようになっていたかをユーザに通知します。たとえば、トラフィックが「ドロップされていたことが予想される」とマークされる場合があります。この情報をトラフィック分析に使用し、インライン モードが望ましいかどうかを判断するのに役立てることができます。

(注) ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードでは、一部のコンテキストに対してモニタ専用モードを設定し、残りのコンテキストに対して通常のインライン モードを設定することはできません。

例

次に、すべての HTTP トラフィックを ASA FirePOWER モジュールに迂回させ、何らかの理由でモジュールで障害が発生した場合にはすべての HTTP トラフィックをブロックする例を示します。

```
ciscoasa(config)# access-list ASASFR permit tcp any any eq port 80
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list ASASFR
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-close
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

次に、10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛てのすべての IP トラフィックを ASA FirePOWER モジュールに迂回させ、何らかの理由でモジュールに障害が発生してもすべてのトラフィックを許可する例を示します。

```
ciscoasa(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list my-sfr-acl
ciscoasa(config)# class-map my-sfr-class2
ciscoasa(config-cmap)# match access-list my-sfr-acl2
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap)# class my-sfr-class2
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap-c)# service-policy my-sfr-policy interface outside
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
class-map	ポリシー マップ用にトラフィックを識別します。
hw-module module reload	モジュールをリロードします。
hw-module module reset	リセットを実行してから、モジュールをリロードします。
hw-module module shutdown	モジュールをシャットダウンします。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show asp table classify domain sfr	トラフィックを ASA FirePOWER モジュールに送信するために作成された NP ルールを表示します。
show module	モジュールのステータスを表示します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。
sw-module module sfr reload	ソフトウェア モジュールをリロードします。

コマンド	説明
sw-module module sfr reset	ソフトウェア モジュールをリセットします。
sw-module module sfr recover	ソフトウェア モジュール ブート イメージをインストールします。
sw-module module sfr shutdown	ソフトウェア モジュールをシャットダウンします。

shape

QoS トラフィック シェーピングをイネーブルにするには、クラス コンフィギュレーション モードで **shape** コマンドを使用します。ASA などの、ファスト イーサネットを使用してパケットを高速に送信するデバイスが存在し、そのデバイスがケーブル モデムなどの低速デバイスに接続されている場合、ケーブル モデムがボトルネックとなり、ケーブル モデムでパケットが頻繁にドロップされます。さまざまな回線速度を持つネットワークを管理するために、低い固定レートでパケットを送信するように ASA を設定できます。これを *トラフィック シェーピング*と呼びます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

(注) トラフィック シェーピングは、ASA 5505、5510、5520、5540、および 5550 のみでサポートされます。(ASA 5500-X などの)マルチコア モデルでは、シェーピングをサポートしていません。

shape average *rate* [*burst_size*]

no shape average *rate* [*burst_size*]

構文の説明

average *rate*	一定期間におけるトラフィックの平均レート(ビット/秒)を 64000 ～ 154400000 の範囲で設定します。8000 の倍数の値を指定します。期間の計算方法の詳細については、「使用上のガイドライン」の項を参照してください。
burst_size	一定期間において送信可能な平均バースト サイズ(ビット単位)を 2048 ～ 154400000 の範囲で設定します。128 の倍数の値を指定します。*burst_size* を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット/秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 になります。

デフォルト

burst_size を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット/秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 になります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが追加されました。

使用上のガイドライン

トラフィック シェーピングをイネーブルにするには、Modular Policy Framework を使用します。

1. **policy-map**:**class-default** クラス マップに関連付けるアクションを指定します。
   a. **class class-default**:アクションを実行する **class-default** クラス マップを指定します。
   b. **shape**:トラフィック シェーピングをクラス マップに適用します。
   c. （任意）**service-policy**:シェーピングされたトラフィックのサブセットに対してプライオリティ キューイングを適用できるように、**priority** コマンドを設定した異なるポリシー マップを呼び出します。
2. **service-policy**:ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

トラフィック シェーピングの概要

トラフィック シェーピングは、デバイスとリンクの速度を一致させることで、ジッタや遅延の原因になる可能性のあるパケット損失、可変遅延、およびリンク飽和を制御するために使用されます。

- トラフィック シェーピングは、物理インターフェイスのすべての発信トラフィック、または ASA 5505 の場合は VLAN 上のすべての発信トラフィックに適用する必要があります。特定のタイプのトラフィックにはトラフィック シェーピングを設定できません。
- トラフィック シェーピングは、パケットがインターフェイスで送信する準備ができている場合に実装されます。そのため、レートの計算は、IPSec ヘッダーや L2 ヘッダーなどの潜在的なすべてのオーバーヘッドを含む、送信されるパケットの実際のサイズに基づいて実行されます。
- シェーピングされるトラフィックには、through-the-box トラフィックと from-the-box トラフィックの両方が含まれます。
- シェープ レートの計算は、標準トークン バケット アルゴリズムに基づいて行われます。トークン バケット サイズは、バースト サイズ値の 2 倍です。トークン バケットの詳細については、CLI 設定ガイドを参照してください。
- バースト性のトラフィックが指定されたシェープ レートを超えると、パケットはキューに入れられて、後で送信されます。次に、シェーピング キューのいくつかの特性について説明します（階層型プライオリティ キューイングの詳細については、**priority** コマンドを参照してください）。
  - キューのサイズは、シェープ レートに基づいて計算されます。キューは、1500 バイトのパケットとして 200 ミリ秒に相当するシェープ レート トラフィックを保持できます。最小キュー サイズは 64 です。
  - キューの制限に達すると、パケットはキューの末尾からドロップされます。
  - OSPF Hello パケットなどの一部の重要なキープアライブ パケットは、ドロップされません。
  - 時間間隔は、*time_interval = burst_size / average_rate* によって求められます。時間間隔が長くなるほど、シェープ トラフィックのバースト性は高くなり、リンクのアイドル状態が長くなる可能性があります。この効果は、次のような誇張した例を使うとよく理解できます。

平均レート = 1000000

バースト サイズ = 1000000

この例では、時間間隔は 1 秒であり、これは、100 Mbps の FE リンクでは 1 Mbps のトラフィックを時間間隔 1 秒の最初の 10 ミリ秒内にバースト送信できることを意味し、残りの 990 ミリ秒間はアイドル状態になって、次の時間間隔になるまでパケットを送信できません。したがって、音声トラフィックのように遅延が問題になるトラフィックがある場合は、バースト サイズを平均レートと比較して小さくし、時間間隔を短くする必要があります。

QoS 機能の相互作用のしくみ

ASA で必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能を ASA に設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

  同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

- トラフィック シェーピング（1 つのインターフェイス上のすべてのトラフィック）+ 階層型プライオリティ キューイング（トラフィックのサブセット）。

同じインターフェイスに対して、トラフィック シェーピングと標準プライオリティ キューイングを設定することはできません。階層型プライオリティ キューイングのみを設定できます。たとえば、グローバル ポリシーに標準プライオリティ キューイングを設定して、特定のインターフェイスにトラフィック シェーピングを設定する場合、最後に設定した機能は拒否されます。これは、グローバル ポリシーがインターフェイス ポリシーと重複するためです。

通常、トラフィック シェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定は ASA では制限されていません。

例

次の例では、外部インターフェイスのすべてのトラフィックでトラフィック シェーピングをイネーブルにして、DSCP ビットが ef に設定された VPN tunnel-grp1 内のトラフィックにプライオリティを付けます。

```
ciscoasa(config)# class-map TG1-voice
ciscoasa(config-cmap)# match tunnel-group tunnel-grp1
ciscoasa(config-cmap)# match dscp ef

ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class TG1-voice
ciscoasa(config-pmap-c)# priority

ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy

ciscoasa(config-pmap-c)# service-policy shape_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップ内でアクションを実行するクラス マップを指定します。
police	QoS ポリシングをイネーブルにします。
policy-map	サービス ポリシーのトラフィックに適用するアクションを指定します。
priority	QoS プライオリティ キューイングを有効にします。
service-policy（クラス）	階層型ポリシー マップを適用します。
service-policy（グローバル）	サービス ポリシーをインターフェイスに適用します。
show service-policy	QoS 統計情報を表示します。

share-ratio

マッピングアドレスおよびポート(MAP)ドメイン内の基本マッピングルールでポートルールのポート数を決定するポート比率を設定するには、MAP ドメインの基本マッピング ルール コンフィギュレーション モードで **share-ratio** コマンドを使用します。比率を削除するには、このコマンドの **no** 形式を使用します。

share-ratio *number*

no share-ratio *number*

構文の説明

number	プール内に存在する必要があるポートの数。ポート数は 1～65536 の範囲内とし、2 の累乗にする必要があります(1、2、4、8 など)。

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
MAP ドメインの基本マッピング ルール コンフィギュレーション モード。	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが導入されました。

使用上のガイドライン

基本マッピングルールの **start-port** コマンドおよび **share-ratio** コマンドによって、MAP ドメイン内のアドレス変換に使用されるプールの開始ポートとポート数が決まります。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート(MAP)ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート(MAP)ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

show aaa kerberos コマンド～ show asdm sessions コマンド

show aaa kerberos

Kerberos サービス情報を表示するには、特権 EXEC モードで **show aaa kerberos** コマンドを使用します。

show aaa kerberos [**username** *user*] | **keytab**]

構文の説明

keytab	Kerberos キータブファイルに関する情報を表示します。
username *user*	指定されたユーザのチケットを表示します。

デフォルト

キーワードを指定しない場合、すべてのユーザのチケットが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.8(4)	**keytab** キーワードが追加されました。

使用上のガイドライン

ASA にキャッシュされたすべての Kerberos チケットを表示するには、キーワードを指定せずに **show aaa kerberos** コマンドを使用します。特定のユーザの Kerberos チケットを表示するには、**username** キーワードを追加します。キータブファイルに関する情報を表示するには、**keytab** キーワードを使用する必要があります。

例

以下に、**show aaa kerberos** コマンドの使用例を示します。

```
ciscoasa(config)# show aaa kerberos

Default Principal      Valid Starting Expires        Service Principal
kcduser@example.com    06/29/10 17:33:00 06/30/10 17:33:00 asa$/mycompany.com@example.com
kcduser@example.com    06/29/10 17:33:00 06/30/10 17:33:00
http/owa.mycompany.com@example.com
```

次に、Kerberos キータブファイルに関する情報を表示する例を示します。

```
ciscoasa# show aaa kerberos keytab
Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
```

関連コマンド

コマンド	説明
aaa kerberos import-keytab	Kerberos キー発行局（KDC）からエクスポートした Kerberos キータブファイルをインポートします。
clear aaa kerberos	キャッシュされた Kerberos チケットをクリアします。
show running-config aaa-server	AAA サーバの設定を表示します。

show aaa local user

現在ロックされているユーザ名のリストを表示するか、またはユーザ名の詳細を表示するには、グローバル コンフィギュレーション モードで **aaa local user** コマンドを使用します。

show aaa local user [locked]

構文の説明

locked	（任意）現在ロックされているユーザ名のリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

オプションのキーワード **locked** を省略すると、ASA によって、すべての AAA ローカル ユーザの失敗試行およびロックアウト ステータスの詳細が表示されます。

username オプションを使用して単一のユーザを指定するか、**all** オプションを使用してすべてのユーザを指定できます。

このコマンドは、ロックアウトされているユーザのステータスだけに影響します。

管理者をデバイスからロックアウトすることはできません。

例

次に、**show aaa local user** コマンドを使用して、すべてのユーザ名のロックアウト ステータスを表示する例を示します。

次に、制限を 5 回に設定した後に **show aaa local user** コマンドを使用して、すべての AAA ローカル ユーザの失敗した認証試行回数およびロックアウト ステータスの詳細を表示する例を示します。

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
    -                   2       N       mona
    -                   1       N       cisco
    -                   4       N       newuser
ciscoasa(config)#
```

次に、制限を 5 回に設定した後に **lockout** キーワードを指定して **show aaa local user** コマンドを使用し、ロックアウトされている AAA ローカル ユーザのみの失敗した認証試行回数およびロックアウト ステータスの詳細を表示する例を示します。

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	ユーザが何回誤ったパスワードを入力するとロック アウトされるかを示す最大回数を設定します。
clear aaa local user fail-attempts	ロックアウト ステータスを変更しないで、失敗試行回数を 0 にリセットします。
clear aaa local user lockout	指定したユーザまたはすべてのユーザのロックアウト ステータスをクリアして、それらのユーザの失敗試行カウンタを 0 に設定します。

show aaa login-history

ログイン履歴を表示するには、特権 EXEC モードで **show aaa login-history** コマンドを使用します。

show aaa login-history [**user** *name*]

構文の説明

user *name*	(オプション)特定のユーザのログイン履歴を指定します。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。
9.12(1)	出力には、指定したユーザの現在のセッションの特権レベルと前のセッションが含まれます。

使用上のガイドライン

デフォルトでは、1 つ以上の CLI 管理方式(SSH、Telnet、シリアル コンソール)でローカル AAA 認証をイネーブルにした場合、ASA はローカル データベースのユーザ名または AAA サーバからのユーザ名を保存します。ログイン履歴を表示するには、**show aaa login-history** コマンドを使用します。履歴存続期間を設定するには、**aaa authentication login-history** コマンドを参照してください。

ASDM のログインは履歴に保存されません。

ログイン履歴はユニット(装置)ごとに保存されます。フェールオーバーおよびクラスタリング環境では、各ユニットが自身のログイン履歴のみを保持します。

ログインの履歴データは、リロードされると保持されなくなります。

例

次に、ログイン履歴を表示する例を示します。

```
ciscoasa(config)# show aaa login-history
Login history for user:                         cisco
Logins in last   1 days:                        45
Last successful login:                          14:07:28 UTC Aug 21 2018 from
10.86.190.50
```

```
Failures since last login:                          0
Last failed login:                                  None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

関連コマンド

コマンド	説明
aaa authentication login-history	ローカル **username** のログイン履歴を保存します。
password-history	直前の **username** パスワードを保存します。ユーザはこのコマンドを設定できません。
password-policy reuse-interval	**username** パスワードの再利用を禁止します。
password-policy username-check	**username** の名前と一致するパスワードを禁止します。
username	ローカル ユーザを設定します。

show aaa-server

AAA サーバの AAA サーバ統計情報を表示するには、特権 EXEC モードで **show aaa-server** コマンドを使用します。

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

構文の説明

LOCAL	(任意) ローカル ユーザ データベースの統計情報を表示します。
groupname	(任意) グループ内のサーバの統計情報を表示します。
host *hostname*	(任意) グループ内の特定のサーバの統計情報を表示します。
protocol *protocol*	(オプション) 以下からプロトコルを指定して、サーバの統計情報を表示します。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

デフォルトで、すべての AAA サーバ統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	http-form プロトコルが追加されました。
8.0(2)	**aaa-server active** コマンドまたは **fail** コマンドを使用して手動でステータスが変更されたかどうかがサーバ ステータスに表示されるようになりました。

例

次に、**show aaa-server** コマンドの出力例を示します。

```
ciscoasa(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

次の表に、**show aaa-server** コマンドのフィールドの説明を示します。

フィールド	説明
Server Group	**aaa-server** コマンドによって指定されたサーバ グループ名。
Server Protocol	**aaa-server** コマンドによって指定されたサーバ グループのサーバ プロトコル。
Server Address	AAA サーバの IP アドレス。
Server port	ASA および AAA サーバによって使用される通信ポート。RADIUS 認証ポートは、**authentication-port** コマンドを使用して指定できます。RADIUS アカウンティング ポートは、**accounting-port** コマンドを使用して指定できます。非 RADIUS サーバでは、ポートは **server-port** コマンドによって設定されます。
Server status	サーバのステータス。次のいずれかの値が表示されます。 • ACTIVE：ASA はこの AAA サーバと通信します。 • FAILED：ASA はこの AAA サーバと通信できません。この状態になったサーバは、設定されているポリシーに応じて一定期間この状態のままとなった後、再アクティブ化されます。 ステータスの後に「(admin initiated)」と表示されている場合、このサーバは、**aaa-server active** コマンドまたは **fail** コマンドを使用して手動で障害発生状態にされたか、または再アクティブ化されています。 最終トランザクション日時を次の形式で示します。 **Last transaction ({success | failure}) at** *time timezone date* ASA がサーバと通信したことがない場合は、次のメッセージが表示されます。 **Last transaction at Unknown**

フィールド	説明
Number of pending requests	現在進行中の要求数。
Average round trip time	サーバとのトランザクションを完了するまでにかかる平均時間。
Number of authentication requests	ASA によって送信された認証要求数。タイムアウト後の再送信は、この値には含まれません。
Number of authorization requests	認可要求数。この値は、コマンド認可、コンピュータを通過するトラフィック（TACACS+ サーバの場合）の認可、トンネル グループでイネーブルにされた WebVPN および IPsec 認可機能が原因の認可要求を指します。タイムアウト後の再送信は、この値には含まれません。
Number of accounting requests	アカウンティング要求数。タイムアウト後の再送信は、この値には含まれません。
Number of retransmissions	内部タイムアウト後にメッセージが再送信された回数。この値は、Kerberos および RADIUS サーバ（UDP）にのみ適用されます。
Number of accepts	成功した認証要求数。
Number of rejects	拒否された要求数。この値には、エラー状態、および実際にクレデンシャルが AAA サーバから拒否された場合の両方が含まれます。
Number of challenges	最初にユーザ名とパスワードの情報を受信した後に、AAA サーバがユーザに対して追加の情報を要求した回数。
Number of malformed responses	該当なし。将来的な使用のために予約されています。
Number of bad authenticators	次のいずれかが発生した回数。 • RADIUS パケットの「authenticator」ストリングが破損している（まれなケース）。 • ASA の共有秘密キーと RADIUS サーバの共有秘密キーが一致しない。この問題を修正するには、正しいサーバ キーを入力します。 この値は、RADIUS にのみ適用されます。
Number of timeouts	ASA が、AAA サーバが応答しない、または動作が不正であることを検出し、オフラインであると見なした回数。
Number of unrecognized responses	認識できない応答またはサポートしていない応答を ASA が AAA サーバから受信した回数。たとえば、サーバからの RADIUS パケット コードが不明なタイプ（既知の「access-accept」、「access-reject」、「access-challenge」または「accounting-response」以外のタイプ）である場合です。通常、これは、サーバからの RADIUS 応答パケットが破損していることを意味していますが、まれなケースです。

関連コマンド

コマンド	説明
show running-config aaa-server	指定したサーバ グループ内のすべてのサーバ、または特定のサーバの統計情報を表示します。
clear aaa-server statistics	AAA サーバ統計情報をクリアします。

show access-list

アクセス リストのヒット カウンタおよびタイムスタンプ値を表示するには、特権 EXEC モードで **show access-list** コマンドを使用します。

show access-list [*id* [*ip_address* | **brief** | **numeric**] | **element-count**]

構文の説明

brief	(任意)アクセス リスト ID、ヒット カウント、および最終ルール ヒットのタイムスタンプをすべて 16 進形式で表示します。
id	(オプション)既存のアクセス リストの ID のカウンタを表示します。
ip_address	(オプション)指定したアクセスリスト内の送信元 IP アドレスまたはホスト名のカウンタを表示します。
numeric	(任意)ACL 名を指定すると、ポートが名前ではなく数値で表示されます。たとえば、www ではなく 80 と表示されます。
element-count	(任意)システムで定義されているすべてのアクセスリストのアクセス コントロール エントリの総数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	**brief** キーワードのサポートが追加されました。
8.3(1)	ACL タイムスタンプを表示するための ACE 表示パターンが変更されました。
9.14(1)	**numeric** および **element-count** キーワードが追加されました。

使用上のガイドライン

brief キーワードを指定して、アクセス リスト ヒット カウント、ID、およびタイムスタンプ情報を 16 進形式で表示できます。16 進形式で表示されるコンフィギュレーション ID は、3 列に表示され、Syslog 106023 および 106100 で使用されるものと同じ ID です。

アクセス リストが最近変更された場合、リストは出力から除外されます。この場合は、メッセージにそのことが示されます。

(注) 出力には、ACL に含まれる要素の数が表示されます。この番号は、必ずしも ACL 内のアクセス コントロール エントリ (ACE) の数と同じではありません。たとえば、アドレス範囲をもつネットワーク オブジェクトを使用する場合、システムは追加の要素を作成することがありますが、これらの追加要素は出力に含まれません。

クラスタリングのガイドライン

ASA クラスタリングを使用する場合、トラフィックが単一のユニットにより受信された場合でも、クラスタリングのダイレクタ ロジックにより、その他のユニットは ACL のヒット カウントを示す場合があります。これは予期された動作です。クライアントから直接パケットを受信しなかったユニットは、所有者要求に応じてクラスタ制御リンクを介して転送されたパケットを受信することがあるため、ユニットはパケットを受信ユニットに戻す前に ACL をチェックすることがあります。このため、トラフィックがユニットを通過しなかった場合でも ACL ヒット カウントが増分されます。

例

次に、16 進形式で指定されたアクセス ポリシー(ヒット カウントがゼロではない ACE)に関する簡単な情報の例を示します。最初の 2 列には、ID が 16 進形式で表示され、3 番めの列にはヒット カウントがリストされ、4 番めの列には、タイムスタンプ値が 16 進形式で表示されます。ヒット カウントの値は、トラフィックがルールにヒットした回数を表します。タイムスタンプ値は、最終ヒットの時刻を報告します。ヒット カウントがゼロの場合、情報は表示されません。

次に、**show access-list** コマンドの出力例を示します。これは、「IN」方向の outside インターフェイスに適用される、アクセス リスト名「test」を示します。

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1
object-group D1 0x44ae5901
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq telnet (hitcnt=1) 0xca10ca21
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq ssh(hitcnt=1) 0x5b704158
```

次に、**object-group-search** グループがイネーブルになっていない場合の **show access-list** コマンドの出力例を示します。

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group
BLK-LAN 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=10) 0x30fe29a6
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
14.14.14.0 255.255.255.0 (hitcnt=2) 0xce8596ec
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
```

```
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

次に、**object-group-search** グループがイネーブルになっている場合の **show access-list** コマンドの出力例を示します。

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

次に、Telnet トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
```

次に、SSH トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
5b704158 44ae5901 00000001 4a68aaa9
```

次に、**show access-list** コマンドの出力例を示します。これは、ACL 最適化がイネーブルになっている、「IN」方向の outside インターフェイスに適用される、アクセス リスト名「test」を示します。

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1
object-group D1 0x44ae5901
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq
telnet (hitcnt=1) 0x7b1c1660
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq ssh
(hitcnt=1) 0x3666f922
```

次に、Telnet トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
```

次に、SSH トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922 44ae5901 00000001 4a68ab66
```

次に、システムで定義されているすべてのアクセスリストのアクセス コントロール エントリの総数である要素カウントの例を示します。アクセスグループとして割り当てられているアクセスリストの場合、アクセスをグローバルに、またはインターフェイス上で制御するために、**object-group-search access-control** コマンドを使用してオブジェクトグループ検索をイネーブルにすることで、要素カウントを減らすことができます。オブジェクトグループ検索をイネーブルにすると、ネットワークオブジェクトがアクセス コントロール エントリで使用されます。それ以外の場合、オブジェクトはそのオブジェクトに含まれる個々の IP アドレスに展開され、送信元/宛先アドレスのペアごとに個別のエントリが書き込まれます。したがって、5 つの IP アドレスを持つ送信元ネットワークオブジェクトと 6 つのアドレスを持つ宛先オブジェクトを使用する単一のルールは、1 つではなく 30 の要素（5 x 6 エントリ）に展開されます。要素カウントが多いほど、アクセスリストが大きくなり、パフォーマンスに影響を与える可能性が高くなります。

```
asa(config)# show access-list element-count
Total number of access-list elements: 33934
```

関連コマンド

コマンド	説明
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
clear access-list	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

show activation-key

永続ライセンス、アクティブな時間ベースのライセンス、および永続ライセンスとアクティブな時間ベースのライセンスの組み合わせである実行ライセンスを表示するには、特権 EXEC モードで **show activation-key** コマンドを使用します。フェールオーバー ユニットでは、このコマンドによって、プライマリおよびセカンダリ ユニットの結合キーである、「フェールオーバー クラスタ」ライセンスも表示されます。

show activation-key [detail]

構文の説明

detail	非アクティブな時間ベース ライセンスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(4)	**detail** キーワードが追加されました。
8.2(1)	出力が変更されて、追加のライセンス情報が含まれるようになりました。
8.3(1)	出力に、機能で使用されるのが永続キーまたは時間ベース キーのいずれであるか、および使用中の時間ベース キーの期間が含まれるようになりました。インストールされているすべての時間ベース キー（アクティブと非アクティブの両方）も表示されます。
8.4(1)	ペイロード暗号化機能のないモデルのサポートが追加されました。

使用上のガイドライン

一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。表 2-1 に、リロードが必要なライセンスを示します。

表 2-1　永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
すべてのモデル	暗号化ライセンスのダウングレード
ASAv	vCPU ライセンスのダウングレード。

リロードが必要な場合は、**show activation-key** 出力は次のようになります。

```
The flash activation key is DIFFERENT from the running key.

The flash activation key takes effect after the next reload.
```

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN およびユニファイド コミュニケーション ライセンスはリストに示されません。

例

例 2-1　show activation-key コマンドのスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、およびアクティブな各時間ベース ライセンスを示す、スタンドアロン ユニットの **show activation-key** コマンドの出力例を示します。

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

例 2-2　show activation-key detail のスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、および永続ライセンスとインストールされている各時間ベース ライセンス（アクティブおよび非アクティブ）を示す、スタンドアロン ユニットの **show activation-key detail** コマンドの出力例を示します。

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5505 Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days
```

```
Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

例 2-3　show activation-key detail のフェールオーバー ペアのプライマリ ユニットの出力

次に、プライマリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットの永続ライセンス。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4           perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
```

```
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                   : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

例 2-4　show activation-key detail のフェールオーバー ペアのセカンダリ ユニットの出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。

- セカンダリ ユニットの永続ライセンス。
- セカンダリのインストール済みの時間ベース ライセンス(アクティブおよび非アクティブ)。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
```

```
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                    : Disabled       perpetual
Security Contexts               : 2              perpetual
GTP/GPRS                        : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

例 2-5　show activation-key のライセンスがない ASAv のスタンドアロン ユニットの出力

展開した 1 つの vCPU ASAv の次の出力は、空白のアクティベーション キー、ライセンスなしの状態、1 つの vCPU ライセンスをインストールするメッセージを示しています。

(注) このコマンド出力には「This platform has an ASAv VPN Premium license.」が表示されます。このメッセージは、ASAv がペイロード暗号化を実行できることを示しており、ASAv の標準ライセンスと Premium ライセンスを参照しません。

```
ciscoasa# show activation-key
Serial Number:  9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Virtual CPUs                    : 0              perpetual
Maximum Physical Interfaces     : 10             perpetual
Maximum VLANs                   : 50             perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Standby perpetual
Encryption-DES                  : Enabled        perpetual
Encryption-3DES-AES             : Enabled        perpetual
Security Contexts               : 0              perpetual
GTP/GPRS                        : Disabled       perpetual
AnyConnect Premium Peers        : 2              perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                 : 250            perpetual
Total VPN Peers                 : 250            perpetual
Shared License                  : Disabled       perpetual
AnyConnect for Mobile           : Disabled       perpetual
AnyConnect for Cisco VPN Phone  : Disabled       perpetual
Advanced Endpoint Assessment    : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Enabled        perpetual
```

```
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.
```

例 2-6　show activation-key の vCPU 標準ライセンスを 4 つ所有する ASAv のスタンドアロンユニットの出力

(注)　このコマンド出力には「This platform has an ASAv VPN Premium license.」が表示されます。このメッセージは、ASAv がペイロード暗号化を実行できることを示しており、ASAv の標準ライセンスと Premium ライセンスを参照しません。

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
```

例 2-7　show activation-key の vCPU Premium ライセンスを 4 つ所有する ASAv のスタンドアロンユニットの出力

(注)　このコマンド出力には「This platform has an ASAv VPN Premium license.」が表示されます。このメッセージは、ASAv がペイロード暗号化を実行できることを示しており、ASAv の標準ライセンスと Premium ライセンスを参照しません。

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 750            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

例 2-8　show activation-key のフェールオーバー ペアでの ASA サービス モジュール プライマリ ユニットの出力

次に、プライマリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
```

```
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

例 2-9　show activation-key のフェールオーバー ペアでの ASA サービス モジュール セカンダリ ユニットの出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
```

```
Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

例 2-10 クラスタでの show activation-key の出力

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
```

```
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 The flash permanent activation key is the SAME as the running permanent key.


Serial Number:  JMX1232L11M
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Running Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited  perpetual
Maximum VLANs                : 50         perpetual
Inside Hosts                 : Unlimited  perpetual
Failover                     : Disabled   perpetual
VPN-DES                      : Enabled    perpetual
VPN-3DES-AES                 : Enabled    perpetual
Security Contexts            : 0          perpetual
GTP/GPRS                     : Disabled   perpetual
SSL VPN Peers                : 2          perpetual
Total VPN Peers              : 250        perpetual
Shared License               : Disabled   perpetual
AnyConnect for Mobile        : Disabled   perpetual
AnyConnect for Linksys phone : Disabled   perpetual
AnyConnect Essentials        : Enabled    perpetual
Advanced Endpoint Assessment : Disabled   perpetual
UC Phone Proxy Sessions      : 12         62 days
Total UC Proxy Sessions      : 12         62 days
Botnet Traffic Filter        : Enabled    646 days

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Botnet Traffic Filter        : Enabled    646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
SSL VPN Peers           : 100         108 days
```

関連コマンド

コマンド	説明
activation-key	アクティベーション キーを変更します。

show ad-groups

Active Directory サーバにリストされているグループを表示するには、特権 EXEC モードで **show ad-groups** コマンドを使用します。

show ad-groups *name* **[filter** ***string*****]**

構文の説明

name	問い合わせる Active Directory サーバ グループの名前。
string	検索するグループ名の全体または一部を指定する、引用符で囲んだ問い合わせに含めるストリング。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

show ad-groups コマンドは、グループの取得に LDAP プロトコルを使用する Active Directory サーバに対してのみ適用されます。このコマンドを使用して、ダイナミック アクセス ポリシー AAA 選択基準に使用できる AD グループを表示します。

LDAP 属性タイプが LDAP の場合、ASA がサーバからの応答を待機するデフォルト時間は 10 秒です。aaa-server ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを実行し、時間を調整できます。

(注) Active Directory サーバに数多くのグループが含まれている場合は、サーバが応答パケットに格納できるデータ量の制限に基づいて **show ad-groups** コマンドの出力が切り捨てられることがあります。この問題を回避するには、**filter** オプションを使用して、サーバからレポートされるグループ数を減らします。

例

```
ciscoasa# show ad-groups LDAP-AD17
Server Group    LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups       46
Account Operators
Administrators
APP-SSL-VPN CIO Users
Backup Operators
Cert Publishers
CERTSVC_DCOM_ACCESS
Cisco-Eng
DHCP Administrators
DHCP Users
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Doctors
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Employees
Engineering
Engineering1
Engineering2
Enterprise Admins
Group Policy Creator Owners
Guests
HelpServicesGroup
```

次に、同じコマンドで **filter** オプションを使用した例を示します。

```
ciscoasa(config)# show ad-groups LDAP-AD17 filter “Eng”
.
Server Group    LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups       4
Cisco-Eng
Engineering
Engineering1
Engineering2
```

関連コマンド

コマンド	説明
ldap-group-base-dn	サーバが、ダイナミック グループ ポリシーで使用されるグループの検索を開始する Active Directory 階層のレベルを指定します。
group-search-timeout	グループのリストについて Active Directory サーバからの応答を ASA が待機する時間を調整します。

show admin-context

現在管理コンテキストとして割り当てられているコンテキスト名を表示するには、特権 EXEC モードで **show admin-context** コマンドを使用します。

show admin-context

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show admin-context** コマンドの出力例を示します。次の例では、「admin」という名前で、フラッシュのルート ディレクトリに保存されている管理コンテキストが表示されています。

```
ciscoasa# show admin-context
Admin: admin flash:/admin.cfg
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
clear configure context	すべてのコンテキストを削除します。
mode	コンテキスト モードをシングルまたはマルチに設定します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

show alarm settings

ISA 3000 で各タイプのアラームの構成を表示するには、ユーザ EXEC モードで **show alarm settings** コマンドを使用します。

show alarm settings

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、**show alarm settings** コマンドの出力例を示します。

```
ciscoasa> show alarm settings
Power Supply
         Alarm                   Disabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Temperature-Primary
         Alarm                   Enabled
         Thresholds              MAX: 92C              MIN: -40C
         Relay                   Enabled
         Notifies                Enabled
         Syslog                  Enabled
Temperature-Secondary
         Alarm                   Disabled
         Threshold
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
```

```
Input-Alarm 1
         Alarm                    Enabled
         Relay                    Disabled
         Notifies                 Disabled
         Syslog                   Enabled
Input-Alarm 2
         Alarm                    Enabled
         Relay                    Disabled
         Notifies                 Disabled
         Syslog                   Enabled
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

show arp

ARP テーブルを表示するには、特権 EXEC モードで **show arp** コマンドを使用します。

show arp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	ダイナミック ARP の期間経過が表示に追加されました。

使用上のガイドライン

表示出力には、ダイナミック、スタティック、およびプロキシ ARP エントリが表示されます。ダイナミック ARP エントリには、ARP エントリの秒単位のエージングが含まれています。エージングの代わりに、スタティック ARP エントリにはダッシュ(-)が、プロキシ ARP エントリには「alias」という状態が含まれています。

例

次に、**show arp** コマンドの出力例を示します。1 つめのエントリは、2 秒間エージングされているダイナミック エントリです。2 つめのエントリはスタティック エントリ、3 つめのエントリはプロキシ ARP のエントリです。

```
ciscoasa# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	ARP パケットを検査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアします。

コマンド	説明
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp-inspection

各インターフェイスの ARP インスペクション設定を表示するには、特権 EXEC モードで **show arp-inspection** コマンドを使用します。

show arp-inspection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	ルーテッド モードのサポートが追加されました。

例

次に、**show arp-inspection** コマンドの出力例を示します。

```
ciscoasa# show arp-inspection
interface                arp-inspection         miss
-------------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss 列には、ARP インスペクションがイネーブルの場合に一致しないパケットに対して実行するデフォルトのアクション（「flood」または「no-flood」）が表示されます。

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	ARP パケットを検査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアします。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp rate-limit

ARP レート制限設定を表示するには、特権 EXEC モードで **show arp rate-limit** コマンドを使用します。

show arp rate-limit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

arp rate-limit 設定を表示するには、このコマンドを使用します。

例

次に、毎秒 10000 として ARP レートを表示する例を示します。

```
ciscoasa# show arp rate-limit
arp rate-limit 10000
```

関連コマンド

コマンド	説明
arp rate-limit	ARP レート制限を設定します。

show arp statistics

ARP 統計情報を表示するには、特権 EXEC モードで show arp statistics コマンドを使用します。

show arp statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show arp statistics** コマンドの出力例を示します。

```
ciscoasa# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

表 2 に、各フィールドの説明を示します。

表 2-2　show arp statistics のフィールド

フィールド	説明
Number of ARP entries	ARP テーブル エントリの合計数。
Dropped blocks in ARP	IP アドレスが対応するハードウェア アドレスに解決されている間にドロップされたブロック数。

表 2-2　show arp statistics のフィールド(続き)

フィールド	説明
Maximum queued blocks	IP アドレスの解決を待機している間に ARP モジュールにキューイングされた最大ブロック数。
Queued blocks	現在 ARP モジュールにキューイングされているブロック数。
Interface collision ARPs received	すべての ASA インターフェイスで受信された、ASA インターフェイスの IP アドレスと同じ IP アドレスからの ARP パケット数。
ARP-defense gratuitous ARPs sent	ARP-Defense メカニズムの一環として ASA によって送信された Gratuitous ARP の数。
Total ARP retries	最初の ARP 要求への応答でアドレスが解決されなかった場合に ARP モジュールによって送信される ARP 要求の合計数。
Unresolved hosts	現在も ARP モジュールによって ARP 要求が送信されている未解決のホスト数。
Maximum unresolved hosts	最後にクリアされた後、または ASA の起動後に、ARP モジュールに存在した未解決ホストの最大数。

関連コマンド

コマンド	説明
arp-inspection	ARP パケットを検査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアして、値をゼロにリセットします。
show arp	ARP テーブルを表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp vtep-mapping

リモート セグメント ドメインにある IP アドレスの VNI インターフェイスでキャッシュされた MAC アドレスとリモート VTEP IP アドレスを表示するには、特権 EXEC モードで **show arp vtep-mapping** コマンドを使用します。

show arp vtep-mapping

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

  手動で複数のピアを定義することはできません。

  ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンド ノードの MAC アドレスを取得します。

- マルチキャスト グループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

  ASA は、IP マルチキャスト パケット内の VXLAN カプセル化 ARP ブロードキャスト パケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

例

show arp vtep-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

show asdm history

ASDM 履歴バッファの内容を表示するには、特権 EXEC モードで **show asdm history** コマンドを使用します。

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

構文の説明

asdmclient	（任意）ASDM クライアント用にフォーマットされた ASDM 履歴データを表示します。
feature *feature*	（任意）履歴表示を指定した機能に制限します。*feature* 引数には、次の値を指定できます。 • **all**：すべての機能の履歴を表示します（デフォルト）。 • **blocks**：システム バッファの履歴を表示します。 • **cpu**：CPU 使用状況の履歴を表示します。 • **failover**：フェールオーバーの履歴を表示します。 • **ids**：IDS の履歴を表示します。 • **interface** *if_name*：指定したインターフェイスの履歴を表示します。*if_name* 引数は、**nameif** コマンドで指定したインターフェイスの名前です。 • **memory**：メモリ使用状況の履歴を表示します。 • **perfmon**：パフォーマンス履歴を表示します。 • **sas**：セキュリティ アソシエーションの履歴を表示します。 • **tunnels**：トンネルの履歴を表示します。 • **xlates**：変換スロット履歴を表示します。
snapshot	（任意）最後の ASDM 履歴データ ポイントのみを表示します。
view *timeframe*	（任意）履歴の表示を指定した期間に制限します。*timeframe* 引数には、次の値を指定できます。 • **all**：履歴バッファ内のすべての内容（デフォルト）。 • **12h**：12 時間 • **5d**：5 日 • **60m**：60 分 • **10m**：10 分

デフォルト

引数またはキーワードを指定しない場合は、すべての機能のすべての履歴情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm history** コマンドから **show asdm history** コマンドに変更されました。

使用上のガイドライン

show asdm history コマンドは、ASDM 履歴バッファの内容を表示します。ASDM 履歴情報を表示する前に、**asdm history enable** コマンドを使用して、ASDM 履歴トラッキングをイネーブルにする必要があります。

例

次に、**show asdm history** コマンドの出力例を示します。このコマンドでは、直近の 10 分間に収集された外部インターフェイスのデータに出力が制限されています。

```
ciscoasa# show asdm history view 10m feature interface outside

Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
```

```
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
ciscoasa#
```

次に、**show asdm history** コマンドの出力例を示します。前の例と同様に、このコマンドでは、直近の 10 分間に収集された外部インターフェイスのデータに出力が制限されています。ただし、この例では、出力は ASDM クライアント用にフォーマットされています。

```
ciscoasa# show asdm history view 10m feature interface outside asdmclient

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|
62469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|
62553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|
62636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|
62723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
...
```

次に、**snapshot** キーワードを使用した **show asdm history** コマンドの出力例を示します。

```
ciscoasa# show asdm history view 10m snapshot

Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
```

```
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
```

```
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
```

```
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPsec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
ciscoasa#
```

関連コマンド

コマンド	説明
asdm history enable	ASDM 履歴トラッキングをイネーブルにします。

show asdm image

現在の ASDM ソフトウェア イメージ ファイルを表示するには、特権 EXEC モードで **show asdm image** コマンドを使用します。

show asdm image

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm image** コマンドから **show asdm image** コマンドに変更されました。

例

次に、**show asdm image** コマンドの出力例を示します。

```
ciscoasa# show asdm image

Device Manager image file, flash:/ASDM
```

関連コマンド

コマンド	説明
asdm image	現在の ASDM イメージ ファイルを指定します。

show asdm log_sessions

アクティブな ASDM ロギング セッション、およびそれらに関連するセッション ID のリストを表示するには、特権 EXEC モードで **show asdm log_sessions** コマンドを使用します。

show asdm log_sessions

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

それぞれのアクティブな ASDM セッションには、1 つ以上の関連する ASDM ロギング セッションがあります。ASDM は、ロギング セッションを使用して、ASA から Syslog メッセージを取得します。各 ASDM ロギング セッションには、一意のセッション ID が割り当てられます。このセッション ID を **asdm disconnect log_session** コマンドで使用して、指定したセッションを終了できます。

（注） 各 ASDM セッションには少なくとも 1 つの ASDM ロギング セッションがあるため、**show asdm sessions** および **show asdm log_sessions** の出力は同じように見えることがあります。

例

次に、**show asdm log_sessions** コマンドの出力例を示します。

```
ciscoasa# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect log_session	アクティブな ASDM ロギング セッションを終了します。

show asdm sessions

アクティブな ASDM セッション、およびそれらに関連するセッション ID のリストを表示するには、特権 EXEC モードで **show asdm sessions** コマンドを使用します。

show asdm sessions

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm sessions** コマンドから **show asdm sessions** コマンドに変更されました。

使用上のガイドライン

アクティブな各 ASDM セッションには、一意のセッション ID が割り当てられます。このセッション ID を **asdm disconnect** コマンドで使用して、指定したセッションを終了できます。

例

次に、**show asdm sessions** コマンドの出力例を示します。

```
ciscoasa# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect	アクティブな ASDM セッションを終了します。

CHAPTER 3

show as-path-access-list コマンド～ show auto-update コマンド

show as-path-access-list

現在のすべての自律システム（AS）パス アクセス リストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show as-path-access-list** コマンドを使用します。

show as-path-access-list [*name*]

構文の説明

name	（オプション）AS パス アクセス リスト名を指定します。

デフォルト

name 引数を指定しない場合、コマンド出力には、すべての AS パス アクセス リストの内容が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、**show as-path-access-list** コマンドの出力例を示します。

```
ciscoasa# show as-path-access-list
AS path access list as-path-acl-1
    deny RTR$
AS path access list as-path-acl-2
    permit 100$
```

表 3-1 に、各フィールドの説明を示します。

表 3-1　show as-path-access-list のフィールド

フィールド	説明
AS パス アクセス リスト	AS パス アクセス リスト名を示します。
deny	正規表現が ASCII 文字列としてのルートの AS パスの表現に一致しなくなってから拒否されたパケット数を示します。
permit	正規表現が ASCII 文字列としてのルートの AS パスの表現に一致してから転送されたパケット数を示します。

show asp cluster counter

クラスタリング環境のグローバル情報またはコンテキストに固有の情報をデバッグするには、特権 EXEC モードで **show asp cluster counter** コマンドを使用します。

show asp cluster counter

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show asp cluster counter コマンドは、グローバル DP カウンタおよびコンテキストに固有の DP カウンタを表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。この情報はデバッグの目的でのみ使用されます。また、情報の出力は変更される可能性があります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp cluster counter** コマンドの出力例を示します。

```
ciscoasa# show asp cluster counter

Global dp-counters:


Context specific dp-counters:

MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show asp drop

高速セキュリティ パスでドロップされたパケットまたは接続をデバッグするには、特権 EXEC モードで **show asp drop** コマンドを使用します。

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

構文の説明

flow [*flow_drop_reason*]	（任意）ドロップされたフロー（接続）を表示します。*flow_drop_reason* 引数を使用して、特定の理由を指定できます。考えられるフローのドロップ理由のリストを表示するには、? を使用します。
frame [***frame_drop_reason***]	（任意）ドロップされたパケットを表示します。*frame_drop_reason* 引数を使用して、特定の理由を指定できます。考えられるフレームのドロップ理由のリストを表示するには、? を使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.0(8)/7.2(4)/8.0(4)	カウンタが最後にクリアされた時間を示すタイムスタンプが出力に含まれます（**clear asp drop** コマンドを参照）。また、説明の横にドロップ理由のキーワードが表示されるため、関連キーワードを使用して簡単に **capture asp-drop** コマンドを使用できます。

使用上のガイドライン

show asp drop コマンドは、高速セキュリティ パスによってドロップされたパケットまたは接続を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、一般的な操作のコンフィギュレーション ガイドを参照してください。この情報はデバッグの目的でのみ使用されます。また、情報の出力は変更される可能性があります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

推奨事項を含む、各ドロップの理由の名称と説明の詳細については、show asp drop コマンドの使用方法 [英語] を参照してください。

例

次に、**show asp drop** コマンドの出力例を示します。タイムスタンプが、カウンタが最後にクリアされた時間を示しています。

```
ciscoasa# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                              3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                          4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                             760
  Expired flow (flow-expired)                                               1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                                 24
  NAT failed (nat-failed)                                               28739
  NAT reverse path failed (nat-rpf-failed)                              22266
  Inspection failure (inspect-fail)                                     19433

Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

関連コマンド

コマンド	説明
capture	パケットをキャプチャします。asp drop コードに基づいてパケットをキャプチャするオプションも含まれています。
clear asp drop	高速セキュリティ パスのドロップ統計情報をクリアします。
show conn	接続に関する情報を表示します。

show asp event dp-cp

データ パスまたは制御パスのイベント キューをデバッグするには、特権 EXEC モードで **show asp event dp-cp** コマンドを使用します。

show asp event dp-cp [**cxsc msg**]

構文の説明

cxsc msg	（オプション）CXSC イベント キューに送信される CXSC イベント メッセージを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.1(3)	ルーティング イベント キュー エントリが追加されました。

使用上のガイドライン

show asp event dp-cp コマンドは、データ パスおよび制御パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。データ パスと制御パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp event dp-cp** コマンドの出力例を示します。

```
ciscoasa# show asp event dp-cp

DP-CP EVENT QUEUE                 QUEUE-LEN  HIGH-WATER
Punt Event Queue                          0        2048
Routing Event Queue                       0           1
Identity-Traffic Event Queue              0          17
General Event Queue                       0           0
Syslog Event Queue                        0        3192
Non-Blocking Event Queue                  0           4
Midpath High Event Queue                  0           0
Midpath Norm Event Queue                  0           0
```

```
SRTP Event Queue                            0           0
HA Event Queue                              0           3
Threat-Detection Event Queue                0           3
ARP Event Queue                             0           3
IDFW Event Queue                            0           0
CXSC Event Queue                            0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt              4005920          0   935295  3070625  4005920       4372
  inspect-sunrp   4005920          0   935295  3070625  4005920       4372
routing               77          0       77        0       77          0
arp-in               618          0      618        0      618          0
identity-traffic    1519          0     1519        0     1519          0
syslog              5501          0     5501        0     5501          0
threat-detection      12          0       12        0       12          0
ips-cplane          1047          0     1047        0     1047          0
ha-msg               520          0      520        0      520          0
cxsc-msg             127          0      127        0      127          0
```

show asp load-balance

ロード バランサ キュー サイズのヒストグラムを表示するには、特権 EXEC モードで **show asp load-balance** コマンドを使用します。

show asp load-balance [**detail**]

構文の説明

detail	(オプション)ハッシュ バケットの詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。

使用上のガイドライン

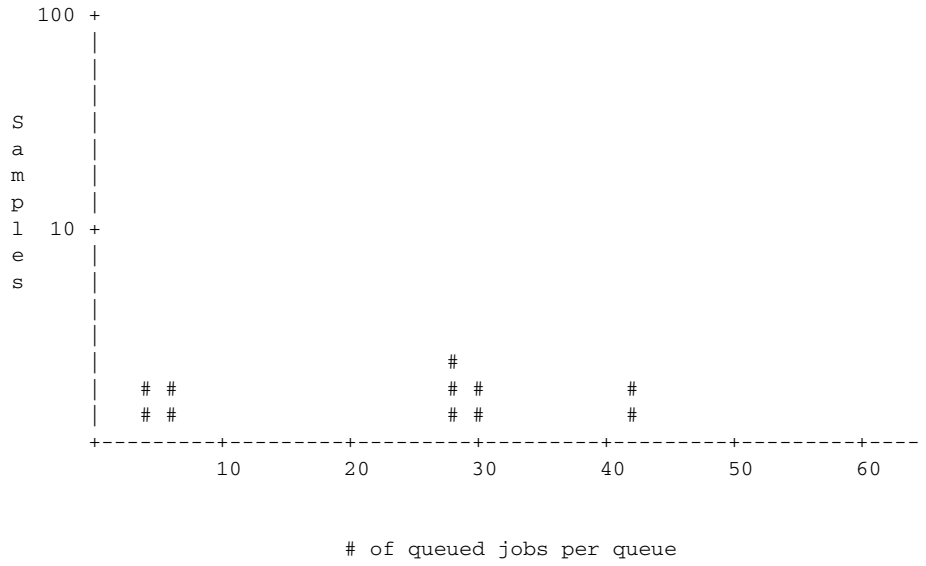
show asp load-balance コマンドは、問題のトラブルシューティングに役立つ場合があります。通常、パケットはインターフェイス受信リングからプルした同じコアによって処理されます。ただし、別のコアが受信したパケットと同じ接続をすでに処理している場合、パケットは、そのコアにキューイングされます。このキューイングによって、他のコアがアイドル状態であっても、ロード バランサ キューが大きくなることがあります。詳細については、**asp load-balance per-packet** コマンドを参照してください。

例

次に、**show asp load-balance** コマンドの出力例を示します。X 軸は異なるキューにキューイングされているパケットの数を表します。Y 軸は、パケットがキューイングされているロード バランサのハッシュ バケットを表します(ヒストグラム バケットを示すヒストグラムのバケットと混同しないでください)。キューを持つハッシュ バケットの正確な数を確認するには、**detail** キーワードを使用します。

```
ciscoasa# show asp load-balance

Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                     ASP load balancer queue sizes
```



次に、**show asp load-balance detail** コマンドの出力例を示します。

```
ciscoasa# show asp load-balance detail

<Same histogram output as before with the addition of the following values for the
histogram>

Data points:
<snip>
  bucket[1-1] = 0 samples
  bucket[2-2] = 0 samples
  bucket[3-3] = 0 samples
  bucket[4-4] = 1 samples
  bucket[5-5] = 0 samples
  bucket[6-6] = 1 samples
<snip>
  bucket[28-28] = 2 samples
  bucket[29-29] = 0 samples
  bucket[30-30] = 1 samples
<snip>
  bucket[41-41] = 0 samples
  bucket[42-42] = 1 samples
```

関連コマンド

コマンド	説明
asp load-balance per-packet	マルチコア ASA モデルのコア ロード バランシング方式を変更します。

show asp load-balance per-packet

パケットごとの ASP ロード バランシングの特定の統計情報を表示するには、特権 EXEC モードで **show asp load-balance per-packet** コマンドを使用します。

show asp load-balance per-packet [history]

構文の説明

history	（オプション）設定ステータス（enabled、disabled、または auto）、現在のステータス（enabled または disabled）、最高水準点と最低水準点、グローバルしきい値、自動切り替えの発生回数、自動スイッチングがイネーブルな場合の最小および最大待機時間、パケットごとの ASP ロード バランシングのタイムスタンプによる履歴、オンおよびオフに切り替える理由を表示します。

デフォルト

このオプションを指定しない場合は、このコマンドによって、基本ステータス、関連する値、およびパケット単位の ASP ロード バランシングの統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

show asp load-balance per-packet コマンドは、パケットごとの ASP ロード バランシングの設定ステータス（enabled、disabled、または auto）、現在のステータス（enabled または disabled）、最高水準点と最低水準点、グローバルしきい値、自動切り替えの発生回数、自動スイッチングがイネーブルな場合の最小および最大待機時間を表示します。

この情報は次の形式で表示されます。

```
Config mode    : [ enabled | disabled | auto ]
Current status : [ enabled | disabled ]

RX ring Blocks low/high watermark      : [RX ring Blocks low watermark in percentage] /
[RX ring Blocks high watermark in percentage]
System RX ring count low threshold     : [System RX ring count low threshold] / [Total
number of RX rings in the system]
System RX ring count high threshold    : [System RX ring count high threshold] / [Total
number of RX rings in the system]
```

auto モード

```
Current RX ring count threshold status : [Number of RX rings crossed watermark] / [Total
number of RX rings in the system]
Number of times auto switched          : [Number of times ASP load-balance per-packet has
been switched]
Min/max wait time with auto enabled    : [Minimal wait time with auto enabled] / [Maximal
wait time with auto enabled] (ms)
```

手動モード

```
Current RX ring count threshold status : N/A
```

ASA 5585-X および ASASM だけがこのコマンドの使用をサポートします。

例

次に、**show asp load-balance per-packet** コマンドの出力例を示します。

```
ciscoasa# show asp load-balance per-packet

Config status  : auto
Current status : disabled

RX ring Blocks low/high watermark      : 50% / 75%
System RX ring count low threshold     : 1 / 33
System RX ring count high threshold    : 7 / 33
Current RX ring count threshold status : 0 / 33
Number of times auto switched          : 17
Min/max wait time with auto enabled    : 200 / 6400 (ms)
```

次に、**show asp load-balance per-packet history** コマンドの出力例を示します。

```
ciscoasa# show asp load-balance per-packet history

Config status  : auto
Current status : disabled

RX ring Blocks low/high watermark      : 50% / 75%
System RX ring count low threshold     : 1 / 33
System RX ring count high threshold    : 7 / 33
Current RX ring count threshold status : 0 / 33
Number of times auto switched          : 17
Min/max wait time with auto enabled    : 200 / 6400 (ms)

==========================================================================================
From State          To State            Reason
==========================================================================================
15:07:13 UTC Dec 17 2013
Manually Disabled   Manually Disabled   Disabled at startup

15:09:14 UTC Dec 17 2013
Manually Disabled   Manually Enabled    Config

15:09:15 UTC Dec 17 2013
Manually Enabled    Auto Disabled       0/33 of the ring(s) crossed the watermark

15:10:16 UTC Dec 17 2013
Auto Disabled       Auto Enabled        1/33 of the ring(s) crossed the watermark
                                        Internal-Data0/0 RX[01] crossed above high watermark

15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        2/33 of the ring(s) crossed the watermark
                                        Internal-Data0/1 RX[04] crossed above high watermark
```

```
15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        3/33 of the ring(s) crossed the watermark
                                        Internal-Data0/1 RX[05] crossed above high watermark

15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        2/33 of the ring(s) crossed the watermark
                                        Internal-Data0/0 RX[01] dropped below low watermark

15:10:17 UTC Dec 17 2013
Auto Enabled        Auto Enabled        3/33 of the ring(s) crossed the watermark
                                        Internal-Data0/2 RX[01] crossed above high watermark

(---More---)

15:14:01 UTC Dec 17 2013
Auto Enabled        Auto Disabled       8/33 of the ring(s) crossed the watermark
                                        Internal-Data0/3 RX[01] crossed above high watermark

15:14:01 UTC Dec 17 2013
Auto Disabled       Auto Enabled        7/33 of the ring(s) crossed the watermark
                                        Internal-Data0/3 RX[01] dropped below low watermark

(---More---)

15:20:11 UTC Dec 17 2013
Auto Enabled        Auto Disabled       0/33 of the ring(s) crossed the watermark
                                        Internal-Data0/2 RX[01] dropped below low watermark
(---More---)
```

関連コマンド

コマンド	説明
asp load-balance per-packet auto	各インターフェイス受信リングまたはフローのセットでのパケットごとの ASP ロード バランシングのオンとオフを自動的に切り替えます。
clear asp load-balance history	パケットごとの ASP ロード バランシングの履歴をクリアし、自動切り替えが発生した回数をリセットします。

show asp table cluster chash-table

クラスタ ハッシュ テーブルを表示するには、特権 EXEC モードで **show asp table cluster chash-table** コマンドを使用します。

show asp table cluster chash-table

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

同じサイト内のトラフィックをディレクタ ローカリゼーションを使用してローカライズするには、各クラスタのメンバー ユニットで 2 つの追加 cHash テーブルを維持します。1 つのテーブルにはローカル サイト内のすべてのメンバーが含まれ、もう 1 つには現在のユニット以外のすべてのローカル メンバーが含まれます。

例

次に、**show asp table cluster chash** コマンドの出力例を示します。サイト 1 にはユニット 0 と 2 があり、サイト 2 には ユニット 1 と 3 があります。次をユニット 0 から表示します。

```
ciscoasa/master# show asp table cluster chash-table

Cluster current chash table:

0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  0,  0,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  0,  0,  0,  0,  0,  0,  0,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,  0,  0,  0,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  0,  0,  0,  0,  0,  0,  0,
```

```
0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  2,  2,
0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  0,  0,  0,
0,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  0,  0,  0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  0,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  0,  0,  0,  0,
0,  0,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  0,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
2,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
2,  2,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  0,  0,  0,  0,  0,  0,
0,  0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  0,  0,  0,  2,  2,  2,  2,  2,  2,  0,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  2,  0,  0,  0,  0,  0,  0,  0,
0,  0,  0,  0,  0,  0,  0,  0,  0,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  0,  0,  0,  2,  2,  2,  2,  0,  0,  0,  0,

Cluster backup chash table:

2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,
2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,  2,

[...]
```

関連コマンド

コマンド	説明
director-localization	ディレクタ ローカリゼーションをイネーブルにします。

show asp table arp

高速セキュリティ パスの ARP テーブルをデバッグするには、特権 EXEC モードで **show asp table arp** コマンドを使用します。

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

構文の説明

address *ip_address*	（任意）ARP テーブル エントリを表示する IP アドレスを指定します。
interface *interface_name*	（任意）ARP テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	（任意）IP アドレスのサブネット マスクを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.8(2)	"reference" 情報のコマンド出力が更新されました。

使用上のガイドライン

show arp コマンドがコントロール プレーンの内容を表示するのに対して、**show asp table arp** コマンドは高速セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。コマンドの出力の参照値は、特定のエントリのフロー数を表します。

例

次に、**show asp table arp** コマンドの出力例を示します。

```
ciscoasa# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0 reference 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638 reference 1
  10.86.194.172                           Active   0001.03cf.9e79 hits 0 reference 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0 reference 0
```

```
  10.86.194.188                           Active   000f.904b.80d7 hits 0 reference 0
Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0 reference 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208 reference 5
```

関連コマンド

コマンド	説明
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show asp table classify

高速セキュリティ パスの分類子テーブルをデバッグするには、特権 EXEC モードで **show asp table classify** コマンドを使用します。

show asp table classify [**interface** *interface_name*] [**crypto** | **domain** *domain_name*] [**hits**] [**match** *regexp*] [**user-statistics**]

構文の説明

crypto	(任意)暗号、暗号解除、および IPSec トンネル フロー ドメインのみを表示します。
domain *domain_name*	(任意)特定の分類子ドメインのエントリを表示します。使用可能なドメインのリストについては、CLI のヘルプを参照してください。
hits	(オプション)0 以外のヒット値を持つ分類子エントリを表示します。
interface *interface_name*	(任意)分類子テーブルを表示する特定のインターフェイスを指定します。
match *regexp*	(オプション)正規表現に一致する分類子エントリを表示します。正規表現にスペースが含まれる場合、引用符を使用します。
user-statistics	(オプション)ユーザおよびグループ情報を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(4)	**hits** オプション、および ASP テーブルのカウンタが最後にクリアされたのがいつかを示すタイムスタンプが追加されました。
8.0(2)	match コンパイルが中止された回数を示すために、新しいカウンタが追加されました。このカウンタは、値が 0 より大きい場合のみ表示されます。
8.2(2)	**match** *regexp* オプションが追加されました。
8.4(4.1)	ASA CX モジュールの **csxc** ドメインおよび **cxsc-auth-proxy** ドメインが追加されました。
9.0(1)	**user-statistics** キーワードが追加されました。出力が更新され、セキュリティ グループ名およびソース タグと宛先タグが追加されました。

リリース	変更内容
9.2(1)	ASA FirePOWER モジュールの sfr ドメインが追加されました。
9.3(1)	出力のセキュリティ グループ タグ(SGT)値が変更されました。タグ値「tag=0」は、「unknow」の予約された SGT 値である 0x0 に完全一致することを示しています。SGT 値「tag=any」は、ルールで考慮する必要がない値を示しています。
9.6(2)	**inspect-m3ua** ドメインが追加されました。

使用上のガイドライン

show asp table classify コマンドは、高速セキュリティ パスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。分類子は、着信パケットのプロパティ(プロトコル、送信元アドレス、宛先アドレスなど)を検査して、各パケットを適切な分類ルールと対応付けます。それぞれのルールには、パケットのドロップや通過の許可など、どのタイプのアクションを実行するかを規定した分類ドメインのラベルが付けられます。表示される情報はデバッグの目的でのみ使用されます。また、出力は変更される可能性があります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table classify** コマンドの出力例を示します。

```
ciscoasa# show asp table classify

Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
...
```

次に、**show asp table classify hits** コマンドの出力例を示します。ヒット カウンタの最後のクリアのレコードが示されています。

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
        hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
        mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
        dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
        hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
        mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
        hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
        mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
        dscp=0x0
```

```
in id=0x48f09e0, priority=1, domain=permit, deny=false
        hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
        mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

次に、レイヤ 2 情報を含む **show asp table classify hits** コマンドの出力例を示します。

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
    hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
    hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=any

.
.
.

Output Table:

L2 - Output Table:

L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
    hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
    hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
    hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
    input_ifc=LAN-SEGMENT, output_ifc=any
```

次に、セキュリティ グループがアクセス リストで指定されていない場合の **show asp table classify** コマンドの出力例を示します。

```
ciscoasa# show asp table classify
in  id=0x7ffedb54cfe0, priority=500, domain=permit, deny=true
        hits=0, user_data=0x6, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=224.0.0.0, mask=240.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=management, output_ifc=any
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show asp table cluster chash-table

高速セキュリティ パスの cHash テーブルをクラスタリング用にデバッグするには、特権 EXEC モードで **show asp table cluster chash-table** コマンドを使用します。

show asp table cluster chash-table

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table cluster chash-table コマンドは、高速セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table cluster chash-table** コマンドの出力例を示します。

```
ciscoasa# show asp table cluster chash-table
Cluster current chash table:

00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
```

```
00002223
33111111
11000112
22332000
00231121
11222220
33330223
31013211
11101111
13111111
11023133
30001100
00000111
12022222
00133333
33222000
00022222
33011333
11110002
33333322
13333030
```

関連コマンド

コマンド	説明
show asp cluster counter	クラスタ データパス カウンタ情報を表示します。

show asp table cts sgt-map

Cisco TrustSec のデータ パスに保持されている IP アドレス セキュリティ グループのテーブル データベースから IP アドレス セキュリティ グループのテーブル マップを表示するには、特権 EXEC モードで **show asp table cts sgt-map** コマンドを使用します。

show asp table cts sgt-map [**address** *ipv4*[*/mask*] | **address** *ipv6*[*/prefix*] | **ipv4** | **ipv6** | **sgt** *sgt*]

構文の説明

address {i*pv4*[*/mask*] */ipv6*[*/prefix*]}	(任意)特定の IPv4 または IPv6 アドレスの IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。ネットワークのマッピングを表示するには IPv4 サブネット マスクまたは IPv6 プレフィックスを含めます。
ipv4	(オプション)IPv4 アドレスのすべての IP アドレス セキュリティ グループのテーブル マップを表示します。
ipv6	(オプション)IPv6 アドレスのすべての IP アドレス セキュリティ グループのテーブル マップを表示します。
sgt *sgt*	(オプション)指定されたセキュリティ グループ テーブルの IP アドレス セキュリティ グループのテーブル マップを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.6(1)	ネットワーク マッピングを表示する機能が追加されました。

使用上のガイドライン

アドレスが指定されていない場合は、データ パスの IP アドレス セキュリティ グループ テーブル データベース内のすべてのエントリが表示されます。また、セキュリティ グループの名前がある場合は、表示されます。

例

次に、**show asp table cts sgt-map** コマンドの出力例を示します。

```
ciscoasa# show asp table cts sgt-map

IP Address                          SGT
================================================
10.10.10.5                          1234:Marketing
10.34.89.12                         5:Engineering
10.67.0.0\16                        338:HR
192.4.4.4                           345:Finance

Total number of entries shown = 4
```

次に、**show asp table cts sgt-map address** コマンドの出力例を示します。

```
ciscoasa# show asp table cts sgt-map address 10.10.10.5

IP Address                          SGT
================================================
10.10.10.5                          1234:Marketing

Total number of entries shown = 1
```

次に、**show asp table cts sgt-map ipv6** コマンドの出力例を示します。

```
ciscoasa# show asp table cts sgt-map ipv6

IP Address                                SGT
============================================================
FE80::A8BB:CCFF:FE00:110                  17:Marketing-Servers
FE80::A8BB:CCFF:FE00:120                  18:Eng-Servers

Total number of entries shown = 2
```

次に、**show asp table cts sgt-map sgt** コマンドの出力例を示します。

```
ciscoasa# show asp table cts sgt-map sgt 17

IP Address                                SGT
============================================
FE80::A8BB:CCFF:FE00:110                  17

Total number of entries shown = 1
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show asp table dynamic-filter

高速セキュリティ パスのボットネット トラフィック フィルタ テーブルをデバッグするには、特権 EXEC モードで **show asp table dynamic-filter** コマンドを使用します。

show asp table dynamic-filter [**hits**]

構文の説明

hits	（オプション）0 以外のヒット値を持つ分類子エントリを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table dynamic-filter コマンドは、高速セキュリティ パス内のボットネット トラフィック フィルタのルールを表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table dynamic-filter** コマンドの出力例を示します。

```
ciscoasa# show asp table dynamic-filter

Context: admin
 Address 10.246.235.42 mask 255.255.255.255 name: example.info
flags: 0x44 hits 0
 Address 10.40.9.250 mask 255.255.255.255 name: bad3.example.com
flags: 0x44 hits 0
 Address 10.64.147.20 mask 255.255.255.255 name: bad2.example.com flags: 0x44
hits 0
 Address 10.73.210.121 mask 255.255.255.255 name: bad1.example.com flags:
0x44 hits 0
 Address 10.34.131.135 mask 255.255.255.255 name: bad.example.com flags:
0x44 hits 0
 Address 10.64.147.16 mask 255.255.255.255 name:
```

```
1st-software-downloads.com flags: 0x44 hits 2
 Address 10.131.36.158 mask 255.255.255.255 name: www.example.com flags: 0x41 hits 0
 Address 10.129.205.209 mask 255.255.255.255 flags: 0x1 hits 0
 Address 10.166.20.10 mask 255.255.255.255 flags: 0x1 hits 0
...
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。

コマンド	説明
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

show asp table filter

高速セキュリティ パスのフィルタ テーブルをデバッグするには、特権 EXEC モードで **show asp table filter** コマンドを使用します。

show asp table filter [**access-list** *acl-name*] [**hits**] [**match** *regexp*]

構文の説明

acl-name	（オプション）指定されたアクセス リストにインストールされたフィルタを指定します。
hits	（オプション）0 以外のヒット値を持つフィルタ ルールを指定します。
match *regexp*	（オプション）正規表現に一致する分類子エントリを表示します。正規表現にスペースが含まれる場合、引用符を使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

フィルタが VPN トンネルに適用されている場合は、フィルタ テーブルにフィルタ ルールが登録されます。トンネルにフィルタが指定されている場合は、暗号化前および複合化後にフィルタ テーブルがチェックされ、内部パケットを許可または拒否するかが決定されます。

例

次に、user1 が接続する前の **show asp table filter** コマンドの出力例を示します。暗黙拒否ルールのみが着信と発信の両方向で IPv4 および IPv6 にインストールされます。

```
ciscoasa# show asp table filter

Global Filter Table:
 in  id=0xd616ef20, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f420, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
```

```
        src ip=::/0, port=0
        dst ip=::/0, port=0
 out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

次に、user1 が接続した後の **show asp table filter** コマンドの出力例を示します。VPN フィルタ ACL は、着信方向に基づいて定義されます。ソースがピアを表し、宛先は内部リソースを表します。発信ルールは着信ルールのソースと宛先を交換することによって生成されます。

```
ciscoasa# show asp table filter

Global Filter Table:
 in  id=0xd682f4a0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd682f460, filter_id=0x2(vpnfilter), protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=21
 in  id=0xd68366a0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd6d89050, filter_id=0x2(vpnfilter), protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=5001
 in  id=0xd45d5b08, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d5ac8, filter_id=0x2(vpnfilter), protocol=17
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=5002
 in  id=0xd6244f30, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd6244ef0, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=0
 in  id=0xd64edca8, priority=12, domain=vpn-user, deny=true
        hits=0, user_data=0xd64edc68, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f018, priority=11, domain=vpn-user, deny=true
        hits=43, user_data=0xd613eb58, filter_id=0x0(-implicit deny-), protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f518, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd615f068, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
 out id=0xd7395650, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd7395610, filter_id=0x2(vpnfilter), protocol=6
        src ip=95.1.224.100, mask=255.255.255.255, port=21
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d49b8, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d4978, filter_id=0x2(vpnfilter), protocol=6
        src ip=95.1.224.100, mask=255.255.255.255, port=5001
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d5cf0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d5cb0, filter_id=0x2(vpnfilter), protocol=17
        src ip=95.1.224.100, mask=255.255.255.255, port=5002
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd6245118, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd62450d8, filter_id=0x2(vpnfilter), protocol=1
        src ip=95.1.224.100, mask=255.255.255.255, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
```

```
out id=0xd64ede90, priority=12, domain=vpn-user, deny=true
        hits=0, user_data=0xd64ede50, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f298, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd614d9f8, filter_id=0x0(-implicit deny-), protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f7c8, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161730, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。
show asp table classifier	高速セキュリティ パスの分類子の内容を表示します。

show asp table interfaces

高速セキュリティ パスのインターフェイス テーブルをデバッグするには、特権 EXEC モードで **show asp table interfaces** コマンドを使用します。

show asp table interfaces

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table interfaces コマンドは、高速セキュリティ パスのインターフェイス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table interfaces** コマンドの出力例を示します。

```
ciscoasa# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
```

```
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show asp table routing management-only

高速セキュリティ パスのルーティング テーブルをデバッグするには、特権 EXEC モードで **show asp table routing** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。management-only キーワードは、管理ルーティング テーブル内のナンバー ポータビリティ ルートを表示します。

show asp table routing [**input** | **output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*] management-only

構文の説明

address *ip_address*	ルーティング エントリを表示する IP アドレスを設定します。IPv6 アドレスの場合は、スラッシュ(/)に続けてプレフィックス(0 ～ 128)を入力し、サブネット マスクを含めることができます。たとえば、次のように入力します。 `fe80::2e0:b6ff:fe01:3b7a/128`
input	入力ルート テーブルにあるエントリを表示します。
interface *interface_name*	(任意)ルーティング テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	IPv4 アドレスの場合は、サブネット マスクを指定します。
output	出力ルート テーブルにあるエントリを表示します。
management-only	管理ルーティング テーブル内のナンバー ポータビリティ ルートを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(2)	ゾーンごとのルーティング情報が追加されました。
9.5(1)	管理ルーティング テーブルをサポートするため management-only キーワードが追加されました。

使用上のガイドライン

show asp table routing コマンドは、高速セキュリティ パスのルーティング テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。management-only キーワードは、管理ルーティング テーブル内のナンバー ポータビリティ ルートを表示します。

(注) 無効なエントリが、ASA 5505 で show asp table routing コマンドの出力に表示される場合があります。

例

次に、**show asp table routing** コマンドの出力例を示します。

```
ciscoasa# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

(注) **show asp table routing** コマンドの出力の無効なエントリが ASA 5505 プラットフォームに表示される場合があります。これらのエントリは無視します。これらのエントリは無効です。

関連コマンド

コマンド	説明
show route	コントロール プレーン内のルーティング テーブルを表示します。

show asp table socket

高速セキュリティ パスのソケット情報をデバッグするには、特権 EXEC モードで **show asp table socket** コマンドを使用します。

show asp table socket [**socket handle**] [**stats**]

構文の説明

socket handle	ソケットの長さを指定します。
stats	高速セキュリティ パスのソケット テーブルの統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

show asp table socket コマンドは、高速セキュリティ パスのソケット情報を表示します。この情報は、高速セキュリティ パスのソケットにおける問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table socket** コマンドの出力例を示します。

```
Protocol  Socket    Local Address              Foreign Address          State
TCP       00012bac  10.86.194.224:23           0.0.0.0:*                LISTEN
TCP       0001c124  10.86.194.224:22           0.0.0.0:*                LISTEN
SSL       00023b84  10.86.194.224:443          0.0.0.0:*                LISTEN
SSL       0002d01c  192.168.1.1:443            0.0.0.0:*                LISTEN
DTLS      00032b1c  10.86.194.224:443          0.0.0.0:*                LISTEN
SSL       0003a3d4  0.0.0.0:443                0.0.0.0:*                LISTEN
DTLS      00046074  0.0.0.0:443                0.0.0.0:*                LISTEN
TCP       02c08aec  10.86.194.224:22           171.69.137.139:4190      ESTAB
```

次に、ハンドルありの **show asp table socket** コマンドの出力例を示します。

```
docs-bxb-asa1/NoCluster/actNoFailover# show asp table socket 123456


Statistics for socket 0x00123456:

2) AM Module
   Mod handle: 0x000000000040545a
   Rx:  0/3  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/3  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        App Flow-Ctrl Tx: 0
        Stack:          0x00007fac1cb539c0
        New Conn Cb:    0x0000560fabeeb110
        Notify   Cb:    0x0000560fabeeb500
        App Hdl:        0x00007fac28dcb150
        Shared  Lock:   0x00007fac1685a280
          Group Lock:   0x00007fac1685a280
          Async Lock:   0x00007fac13099640
        Closed Mod Rx: -1, Tx: 3
        Push Module:    INVALID
        State:          LISTEN
        Flags: 0x0
          none

1) SSL Module
   Mod handle: 0x0000000000xxxxxx
   Rx:  0/10 ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/10 ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        Upstream Active/peak/total:     0/0/0
        Downstream Active/peak/total:   0/0/0
        Inbound bytes rx/tx:    0/0
        Inbound packets rx/tx:  0/0
        Inbound packets lost:   0
        Outbound bytes rx/tx:   0/0
        Outbound packets rx/tx: 0/0
        Outbound packets lost:  0
        Upstream Close Attempt:         0
        Upstream Close Forced:          0
        Upstream Close Next:            0
        Upstream Close Handshake:       0
        Downstream Close Attempt:       0
        Downstream Close Forced:        0
        Downstream Close Next:          0
        Inbound discard empty buf:      0
        Empty downstream buf:   0
        Encrypt call:           0
        Encrypt call error:     0
        Encrypt handoff:        0
        Encrypt CB success:     0
        Encrypt CB fail:        0
        Flowed Off:             0
        Stats Last State:       0x0 (UNKWN )
        Pending crypto cmds:    0
        Socket Last State:      0x6000 (UNKWN )
        Socket Read State:      0xf0 (read header)
        Handle Read State:      0xf0 (read header)
        References:             NO Session
        In Rekey:               0x0
        Flags:                  0x0
        Header Len:             5
        Record Type:            0x0
        Record Len:             0
```

```
        Queued Blocks:          0
        Queued Bytes:           0

0) TM Module
   Mod handle: 0x0000000000xxxxxx
   Rx:  0/1  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/1  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        Transp Flow-Ctrl Rx: 0
        TCP handle: 0x0000xxxxxxxxxxxx, Interface inside (0x2)
        Connection state is LISTEN
        Local host: 0.0.0.0, Local port: 2444
        Foreign host: 0.0.0.0, Foreign port: 0
        Client host: 0.0.0.0, Client port: 0
        TTL Inbound: 0, TTL Outbound: 255
        Datagrams (MSS: send 536, receive 0):
          Retransmit Queue:     0
          Input Queue:          0
          mis-ordered:          0 (0 bytes)
          Rcvd:                 0
            out of order:       0
            with data:          0
            min ttl drop:       0
            total data bytes:   0
          Sent:                 0
            retransmit:         0
            fastretransmit:     0
            partialack:         0
            Second Congestion:  0
            with data:          0
            total data bytes:   0
```

次に、**show asp table socket stats** コマンドの出力例を示します。

```
TCP Statistics:
  Rcvd:
     total14794
     checksum errors0
     no port0
  Sent:
     total0

UDP Statistics:
  Rcvd:
     total0
     checksum errors0
  Sent:
     total0
     copied0

NP SSL System Stats:
  Handshake Started:33
  Handshake Complete:33
  SSL Open:4
  SSL Close:117
  SSL Server:58
  SSL Server Verify:0
  SSL Client:0
```

TCP/UDP 統計情報は、送受信したパケットのうち、ASA で実行またはリッスンしているサービス（Telnet、SSH、HTTPS など）に転送されるパケットの数を示すパケット カウンタです。チェックサム エラーは、計算されたパケット チェックサムがパケットに保存されているチェックサム値と一致しなかった（つまり、パケットが破損した）ため、ドロップされたパケットの数です。NP SSL 統計情報は、受信した各タイプのメッセージの数を示します。ほとんどが、SSL サーバまたは SSL クライアントへの新しい SSL 接続の開始と終了を示します。

関連コマンド

コマンド	説明
show asp table vpn-context	高速セキュリティ パスの VPN コンテキスト テーブルを表示します。

show asp table vpn-context

高速セキュリティ パスの VPN コンテキスト テーブルをデバッグするには、特権 EXEC モードで **show asp table vpn-context** コマンドを使用します。

show asp table vpn-context [**detail**]

構文の説明

detail	（任意）VPN コンテキスト テーブルに関する追加の詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(4)	トンネルのドロップ後にステートフル フローを保持する各コンテキストの +PRESERVE フラグが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.13(1)	デバッグ機能を強化するため、次の vpn コンテキスト カウンタが出力に追加されました。 • **Lock Err**: このカウンタは、VPN コンテキスト ロックを取得できなかった場合に増加し、このエラーが発生した回数を示します。 • **No SA**: このカウンタは、VPN コンテキストが処理するパケットを受信したものの、それに対応するアクティブな SA が関連付けられていない場合に増加します。 • **Ip Ver Err**: このカウンタは、不明なバージョンの IP パケットを受信すると増加します。 • **Tun Down**: VPN コンテキストに関連付けられているトンネルが削除されたか、トンネル ハンドルが無効であることを示します。

使用上のガイドライン

show asp table vpn-context コマンドは、高速セキュリティ パスの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table vpn-context** コマンドの出力例を示します。

```
ciscoasa# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

次に、PRESERVE フラグで示されているように固定の IPsec トンネル フロー機能がイネーブルになっている場合の **show asp table vpn-context** コマンドの出力例を示します。

```
ciscoasa(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

次に、**show asp table vpn-context detail** コマンドの出力例を示します。

```
ciscoasa# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
```

```
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

次に、PRESERVE フラグで示されているように固定の IPsec トンネル フロー機能がイネーブルになっている場合の **show asp table vpn-context detail** コマンドの出力例を示します。

```
ciscoasa(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
ciscoasa(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show asp table zone

高速セキュリティ パスのゾーン テーブルをデバッグするには、特権 EXEC モードで **show asp table zone** コマンドを使用します。

show asp table zone [*zone_name*]

構文の説明

zone_name	(オプション)ゾーン名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

show asp table zone コマンドは、高速セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、CLI 設定ガイドを参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table zone** コマンドの出力例を示します。

```
ciscoasa# show asp table zone

Zone: outside-zone id: 2
 Context: test-ctx
  Zone Member(s) : 2
   outside1       GigabitEthernet0/0
   outside2       GigabitEthernet0/1
```

関連コマンド

コマンド	説明
show asp table routing	デバッグ目的で高速セキュリティ パス テーブルを表示し、各ルートに関連付けられたゾーンを表示します。
show zone	ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。

show attribute

VM 属性エージェントとバインディングに関連する情報を表示するには、EXEC モードで **show attribute** コマンドを使用します。

show attribute [host-map [/all] | object-map [/all] | source-group *agent-name*]

構文の説明

host-map	属性への仮想マシンの IP アドレスの現在のバインディングを表示します。すべての属性のバインディングを確認するには、/all を含めます。たとえば、次のように入力します。 `show attribute host-map /all`
object-map	属性への仮想マシンの IP アドレスの現在のバインディングを表示します。すべての属性のバインディングを確認するには、/all を含めます。たとえば、次のように入力します。 `show attribute host-map /all`
source-group	1 つ以上の属性エージェントの設定および状態を表示します。たとえば、次のように入力します。 `show attribute source-groups` *agent-name*

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォールモード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
EXEC モード	• 対応	• 対応	• 対応	—	—

例

次に、**show attribute** コマンドの出力例を示します。

```
ciscoasa# show attribute host-map /all
IP Address-Attribute Bindings Information
        Source/Attribute                        Value
=========================================================================
VMAgent.custom.role                          'Developer'
     169.254.107.176
     169.254.59.151
     10.15.28.34
     10.15.28.32
     10.15.28.31
     10.15.28.33
```

```
VMAgent.custom.role                          'Build Machine'
     10.15.27.133
     10.15.27.135
     10.15.27.134



ciscoasa# show attribute object-map /all
Network Object-Attribute Bindings Information
Object
        Source/Attribute                       Value
=========================================================================
dev
    VMAgent.custom.role                       'Developer'
build
    VMAgent.custom.role                       'Build Machine'

ciscoasa# show attribute source-group

Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attributes being monitored:
       'custom.role ' (2)
```

show auto-update

Auto Update Server のステータスを表示するには、特権 EXEC モードで **show auto-update** コマンドを使用します。

show auto-update

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

Auto Update Server のステータスを表示するには、このコマンドを使用します。

例

次に、**show auto-update** コマンドの出力例を示します。

```
ciscoasa(config)# show auto-update
Poll period: 720 minutes, retry count: 0, retry period: 5 minutes
Timeout: none
Device ID: host name [ciscoasa]
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update server	Auto Update Server を指定します。

auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

CHAPTER 4

how backup-package コマンド～ show cpu コマンド

show backup-package

Cisco ISA 3000 のバックアップ パッケージのステータスとサマリー情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show backup-package** コマンドを使用します。

show backup-package {**status** {**backup** | **restore**} | **summary**}

(注) このコマンドは、Cisco ISA 3000 アプライアンスにのみ適用されます。

構文の説明

backup | **restore**	表示するステータス情報のタイプを指定します。
status	バックアップ操作または復元操作のいずれかのモード、ロケーション、パスフレーズ、最新の時刻情報を表示します。
summary	バックアップ操作と復元操作の両方のステータス情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

また、グローバル コンフィギュレーション モードでは **show backup-package** コマンドも使用できます。

例

次に、バックアップパッケージのサマリー統計情報を表示する例を示します。

```
ciscoasa# show backup-package summary
    backup mode      : auto
    backup location  : disk3:
    backup passphrase: cisco
    last backup time : Mar 23 2014 22:05:52
    restore mode      : auto
    restore location  : disk3:
    restore passphrase: cisco
    Last restore time : Mar 24 2014 05:07:32
```

show bfd drops

BFD でドロップされたパケットの数を表示するには、グローバル コンフィギュレーション モードで **show bfd drops** コマンドを使用します。

show bfd drops

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、BFD でドロップされたパケットを表示する例を示します。

```
ciscoasa# show bfd drops
BFD Drop Statistics
                        IPV4 IPV6 IPV4-M IPV6-M
Invalid TTL             0    0    0      0
BFD Not Configured      0    0    0      0
No BFD Adjacency        0    0    0      0
Invalid Header Bits     0    0    0      0
Invalid Discriminator   0    0    0      0
Session AdminDown       0    0    0      0
Authen invalid BFD ver  0    0    0      0
Authen invalid len      0    0    0      0
Authen invalid seq      0    0    0      0
Authen failed           0    0    0      0
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

show bfd map

設定済みの BFD マップを表示するには、グローバル コンフィギュレーション モードで **show bfd map** コマンドを使用します。

show bfd map

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、BFD マップを表示する例を示します。

```
ciscoasa# show bfd map
Destination: 40.40.40.2/24
 Source: 50.50.50.2/24
 Template: mh
 Authentication(Type): sha-1
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。

コマンド	説明
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

show bfd neighbors

既存の BFD 隣接関係の詳細なリストを表示するには、グローバル コンフィギュレーション モードで **show bfd neighbors** コマンドを使用します。

show bfd neighbors [client {bgp}| details| interface *interface-name* **| ipv4** *ip-address* **| ipv6** *ipv6-address* **| multihop-ipv4** *ip-address* **| multihop-ipv6** *ipv6-address***]**

構文の説明

クライアント	（オプション）特定のクライアントのネイバーを表示します。
bgp	（オプション）BGP クライアントを表示します。
details	（オプション）各ネイバーのすべての BFD プロトコル パラメータおよびタイマーを表示します。
interface *interface-name*	（オプション）指定されたインターフェイスのネイバーを表示します。
ipv4 *ip-address*	（オプション）指定されたシングルホップ IP ネイバーを表示します。
ipv6 *ipv6-address*	（オプション）指定されたシングルホップ IPv6 ネイバーを表示します。
multihop-ipv4 *ip-address*	（オプション）指定されたマルチホップ IP ネイバーを表示します。
multihop-ipv6 *ipv6-address*	（オプション）指定されたマルチホップ IPv6 ネイバーを表示します。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、BFD 問題をトラブルシューティングできます。

例

次に、BFD ネイバーを表示する例を示します。

```
ciscoasa# show bfd neighbors
OurAddr     NeighAddr    LD/RD  RH     Holdown(mult)     State Int
172.16.10.1 172.16.10.2  1/6    1      260 (3 )          Up    Fa0/1
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd summary	BFD のサマリー情報を表示します。

show bfd summary

BFD のサマリー情報を表示するには、グローバル コンフィギュレーション モードで **show bfd summary** コマンドを使用します。

show bfd summary [client | host | session]

構文の説明

クライアント	(オプション)クライアントの BFD サマリーを表示します。
ホスト	(オプション)セッションの BFD サマリーを表示します。
session	(オプション)プロトコルの BFD サマリーを表示します。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、BFD、BFD クライアント、または BFD セッションのサマリー情報を表示できます。BFD クライアントがピアとのセッションを開始すると、BFD は定期的に BFD 制御パケットをピアに送信します。次のセッションの状態に関する情報が、このコマンドの出力に含まれます。

- Up:別の BFD インターフェイスが BFD 制御パケットに確認応答すると、セッションはアップ状態に移行します。
- Down:データ パスで障害が生じ、BFD が設定された時間内に制御パケットを受信しない場合は、セッションとデータ パスがダウンとして宣言されます。セッションがダウンした場合は、BFD クライアントがトラフィックを再ルーティングするために必要なアクションを実行できるように、BFD が BFD クライアントに通知します。

例

次に、BFD サマリーを表示する例を示します。

```
ciscoasa# show bfd summary
         Session         Up      Down
Total    1               1       0

ciscoasa# show bfd summary session
Protocol                  Session     Up Down
IPV4                      1     1     0
Total                     1     1     0

ciscoasa# show bfd summary client
Client                    Session      Up     Down
BGP                       1       1    0
EIGRP                     1       1    0
Total                     2       2    0
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。

show bgp

Border Gateway Protocol（BGP）ルーティング テーブル内のエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp** コマンドを使用します。

show bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*length*] | **bestpath** | **multipaths** | **subnets**] | **bestpath** | **multipaths**] | **all** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name*]]

構文の説明

ip-address	（オプション）AS パス アクセス リスト名を指定します。
mask	（オプション）指定したネットワークの一部であるホストをフィルタリングまたは照合するためのマスク。
longer-prefixes	（オプション）指定したルートと、より限定的なすべてのルートを表示します。
injected	（オプション）BGP ルーティング テーブルに注入された、より限定的なプレフィックスを表示します。
shorter-prefixes	（オプション）指定したルートと、より限定的でないすべてのルートを表示します。
length	（オプション）プレフィックス長。この引数の値は、0 ～ 32 の数値です。
bestpath	（オプション）このプレフィックスの最適パスを表示します。
multipaths	（オプション）このプレフィックスのマルチパスを表示します。
subnets	（オプション）指定したプレフィックスのサブネット ルートを表示します。
all	（オプション）BGP ルーティング テーブルのすべてのアドレス ファミリ情報を表示します。
prefix-list *name*	（オプション）指定したプレフィックス リストに基づいて出力をフィルタリングします。
pending-prefixes	（オプション）BGP ルーティング テーブルからの削除が保留されているプレフィックスを表示します。
route-map *name*	（オプション）指定したルート マップに基づいて出力をフィルタリングします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

show bgp コマンドは、BGP ルーティング テーブルの内容を表示するために使用します。出力は、特定のプレフィックスのエントリ、特定のプレフィックス長のエントリ、および、プレフィックス リスト、ルート マップ、または条件付きアドバタイズメントを介して注入されたプレフィックスのエントリを表示するようにフィルタリングできます。

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、Cisco IOS XE Release 2.4、およびそれ以降のリリースでは、シスコが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドに続けて、**clear bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。

例

次に、BGP ルーティング テーブルの出力例を示します。

```
Router# show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
```

表 4-1 に、各フィールドの説明を示します。

表 4-1　show bgp のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 • s:テーブルエントリが抑制されます。 • d:テーブルエントリがダンプニングされています。 • h:テーブルエントリの履歴です。 • *:テーブルエントリが有効です。 • >:テーブルエントリがそのネットワークで使用するための最良エントリです。 • i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。 • r:テーブルエントリは RIB 障害です。 • S:テーブルエントリは失効しています。 • m:テーブルエントリには、そのネットワークで使用するためのマルチパスが含まれています。 • b:テーブル エントリには、そのネットワークで使用するためのバックアップパスが含まれています。 • x:テーブル エントリには、ネットワークで使用するための最適外部ルートが含まれています。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 • i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 • e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 • ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	ネットワークエンティティの IP アドレス
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、ルータにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システムメトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システム フィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。
(stale)	指定した自律システムの次のパスがグレースフル リスタート プロセス中に「stale」とマークされたことを示します。

show bgp（4 バイト自律システム番号）：例

次に、BGP ルーティング テーブルの出力例を示します。[Path] フィールドの下に 4 バイト自律システム番号（65536 と 65550）が表示されます。この例では、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、Cisco IOS XE Release 2.4 またはそれ以降のリリースが必要です。

```
RouterB# show bgp

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

show bgp ip-address：例

次に、BGP ルーティング テーブルの 192.168.1.0 エントリに関する情報の出力例を示します。

```
Router# show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

次に、BGP ルーティングテーブルの 10.3.3.3 255.255.255.255 エントリに関する情報の出力例を示します。

```
Router# show bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

表 4-2 に、各フィールドの説明を示します。

表 4-2　show bgp（4 バイト自律システム番号）のフィールド

フィールド	説明
BGP routing table entry fo	ルーティング テーブル エントリの IP アドレスまたはネットワーク番号。
version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
Paths	使用可能なパスの数、およびインストールされた最適パスの数。最適パスが IP ルーティングテーブルに登録されている場合、この行に「Default-IP-Routing-Table」と表示されます。
Multipath	このフィールドは、マルチパス ロード シェアリングがイネーブルの場合に表示されます。このフィールドは、マルチパスが iBGP であるか eBGP であるかを示します。
Advertised to update-groups	アドバタイズメントが処理される各アップデート グループの数。
Origin	エントリの作成元。送信元は IGP、EGP、incomplete のいずれかになります。この行には、設定されたメトリック（メトリックが設定されていない場合は 0）、ローカル プリファレンス値（100 がデフォルト）、およびルートのステータスとタイプ（内部、外部、マルチパス、最適）が表示されます。
Extended Community	このフィールドは、ルートが拡張コミュニティ属性を伝送する場合に表示されます。この行には、属性コードが表示されます。拡張コミュニティに関する情報は後続の行に表示されます。

show bgp all：例

次に、**all** キーワードを指定した **show bgp** コマンドの出力例を示します。設定されたすべてのアドレス ファミリに関する情報が表示されます。

```
Router# show bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
```

```
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

show bgp longer-prefixes：例

次に、**longer-prefixes** キーワードを指定した **show bgp** コマンドの出力例を示します。

```
Router# show bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30         8896         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.1.0         10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.11.0        10.92.72.30        42482         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.14.0        10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.15.0        10.92.72.30         8696         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.16.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.17.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.18.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.19.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
```

show bgp shorter-prefixes：例

次に、**shorter-prefixes** キーワードを指定した **show bgp** コマンドの出力例を示します。8 ビットプレフィックス長を指定しています。

```
Router# show bgp 172.16.0.0/16 shorter-prefixes 8

*> 172.16.0.0         10.0.0.2                               0 ?
*                     10.0.0.2                 0             0 200 ?
```

show bgp prefix-list：例

次に、**prefix-list** キーワードを指定した **show bgp** コマンドの出力例を示します。

```
Router# show bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?

*                   10.0.0.2                 0             0 200 ?
```

show bgp route-map：例

次に、**route-map** キーワードを指定した **show bgp** コマンドの出力例を示します。

```
Router# show bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                             0 ?
*                   10.0.0.2                 0           0 200 ?
```

show bgp all community

特定の Border Gateway Protocol（BGP）コミュニティに属するすべてのアドレス ファミリのルートを表示するには、ユーザ EXEC モードまたは特権 EXEC コンフィギュレーション モードで **show bgp all community** コマンドを使用します。

show bgp all community [*community-number...*[*community-number*]] [**local-as**] [**no-advertise**] [**no-export**] [**exact-match**]

構文の説明

community-number.	（オプション）指定したコミュニティ番号に関連するルートを表示します。 複数のコミュニティ番号を指定できます。範囲は 1 ～ 4294967295 または AA:NN（自律システム:コミュニティ番号（2 バイトの番号））です。
local-as	（オプション）ローカル自律システム外に送信されないルートだけを表示します（ウェルノウン コミュニティ）。
no-advertise	（オプション）ピアにアドバタイズされないルートだけを表示します（ウェルノウン コミュニティ）。
no-export	（オプション）ローカル自律システムの外部にエクスポートされていないルートだけを表示します（ウェルノウン コミュニティ）。
exact-match	（オプション）指定した BGP コミュニティ リストと正確に一致するルートだけを表示します。 **（注）** コマンドのキーワードの可用性はコマンド モードによって異なります。**exact-match** キーワードは、ユーザ EXEC モードでは使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザは、**local-as**、**no-advertise**、**no-export** の各キーワードを任意の順序で入力できます。**bgp all community** コマンドを使用する場合、数値のコミュニティはウェルノウン コミュニティの前に入力してください。

たとえば、次の文字列は無効です。

```
ciscoasa# show bgp all community local-as 111:12345
```

代わりに、次の文字列を使用します。

```
ciscoasa# show bgp all community 111:12345 local-as
```

例

次に、**show bgp all community** コマンドの出力例を示します。ここでは、1、2345、6789012 の各コミュニティを指定しています。

```
ciscoasa# show bgp all community 1 2345 6789012 no-advertise local-as no-export
exact-match

For address family: IPv4 Unicast

BGP table version is 5, local router ID is 30.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network  Next Hop            Metric LocPrf Weight Path
*> 10.0.3.0/24       10.0.0.4                               0 4 3 ?
*> 10.1.0.0/16       10.0.0.4                 0             0 4 ?
*> 10.12.34.0/24     10.0.0.6                 0             0 6 ?
```

表 4-26 に、各フィールドの説明を示します。

表 4-3　show bgp all community のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	BGP コミュニティを表示するように設定されたルータのルータ ID。ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 d：テーブルエントリがダンプニングされています。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブル エントリが内部 BGP セッションを経由して学習されます。
Origin codes	エントリの作成元を示します。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、network ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：外部ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元は不明です。通常、これは、IGP から BGP に再配布されたルートです。

表 4-3　show bgp all community のフィールド(続き)

フィールド	説明
Network	ネットワーク エンティティのネットワーク アドレスおよびネットワーク マスク。アドレスのタイプは、アドレス ファミリによって異なります。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。アドレスのタイプは、アドレス ファミリによって異なります。
Metric	相互自律システム メトリック。このフィールドはあまり使用されません。
LocPrf	**set local-preference** コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。

show bgp all neighbors

すべてのアドレス ファミリのネイバーへの Border Gateway Protocol（BGP）接続に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp all neighbors** コマンドを使用します。

show bgp all neighbors [*ip-address*] [**advertised-routes** | **paths** [*reg-exp*] | **policy** [**detail**] | **received prefix-filter** | **received-routes** | **routes**]

構文の説明

ip-address	（任意）ネイバーの IP アドレスです。この引数を省略すると、すべてのネイバーに関する情報が表示されます。
advertised-routes	（オプション）ネイバーにアドバタイズされたすべてのルートを表示します。
paths *reg-exp*	（オプション）指定したネイバーから学習した自律システム パスを表示します。オプションの正規表現を使用して、出力をフィルタ処理できます。
ポリシー	（オプション）アドレス ファミリごとに、ネイバーに適用されるポリシーを表示します。
detail	（オプション）ルート マップ、プレフィックス リスト、コミュニティ リスト、アクセス コントロール リスト（ACL）、自律システム パス フィルタ リストなどの詳細なポリシー情報を表示します。
received prefix-filter	（オプション）指定したネイバーから送信されたプレフィックス リスト（アウトバウンド ルート フィルタ（ORF））を表示します。
received-routes	（オプション）指定したネイバーから受信したすべてのルートを表示します。
routes	（オプション）受信され、受け入れられるすべてのルートを表示します。このキーワードが入力されたときに表示される出力は、**received-routes** キーワードによって表示される出力のサブセットです。

デフォルト

このコマンドの出力には、すべてのネイバーの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

IPv4 などのアドレス ファミリに固有のネイバー セッションの BGP および TCP 接続情報を表示するには、**show bgp all neighbors** コマンドを使用します。

例

次に、**show bgp all neighbors** コマンドの出力例を示します。

```
ciscoasa# show bgp all neighbors

For address family: IPv4 Unicast
BGP neighbor is 172.16.232.53, remote AS 100, external link
 Member of peer-group internal for session parameters
  BGP version 4, remote router ID 172.16.232.53
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        11
  Default minimum time between advertisement runs is 5 seconds

  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0


Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent:4445 (retransmit: 5), with data: 4445, total data bytes;244128
```

表 4-4 に、各フィールドの説明を示します。

表 4-4　show bgp all neighbor のフィールド

フィールド	説明
For address family	後続のフィールドが参照するアドレス ファミリ。
BGP neighbor	BGP ネイバーの IP アドレスとその自律システム番号。
remote AS	ネイバーの自律システム番号。
external link	外部ボーダー ゲートウェイ プロトコル（eBGP）peerP。
BGP version	リモート ルータとの通信に使用される BGP バージョン。
remote router ID	ネイバーの IP アドレス。
BGP state	この BGP 接続の状態。
up for	ベースとなる TCP 接続が存在している時間（hh:mm:ss 形式）。
Last read	BGP がこのネイバーから最後にメッセージを受信してからの時間（hh:mm:ss 形式）。
hold time	BGP がメッセージを受信せずにこのネイバーとセッションを維持した時間（秒数）。
keepalive interval	キープアライブ メッセージがこのネイバーに転送される間隔（秒数）。
Message statistics	メッセージ タイプごとにまとめられた統計。
InQ depth is	入力キュー内のメッセージ数。
OutQ depth is	出力キュー内のメッセージ数。
Sent	送信されたメッセージの合計数。
Rcvd	受信されたメッセージの合計数。
Opens	送受信されたオープンメッセージ数。
Notifications	送受信された通知（エラー）メッセージ数。
Updates	送受信されたアップデートメッセージ数。
Keepalives	送受信されたキープアライブメッセージ数。
Route Refresh	送受信されたルートリフレッシュ要求メッセージ数。
Total	送受信されたメッセージの合計数。
Default minimum time between...	アドバタイズメント送信の間の時間（秒数）。
Connections established	TCP および BGP 接続が正常に確立した回数。
dropped	有効セッションに障害が発生したか停止した回数。
Last reset	このピアリングセッションが最後にリセットされてからの時間（hh:mm:ss 形式）。リセットがこの行に表示された理由。
External BGP neighbor may be...	BGP 存続可能時間（TTL）セキュリティ チェックがイネーブルであることを示します。ローカルピアとリモートピアをまたぐことができるホップの最大数がこの行に表示されます。
Connection state	BGP ピアの接続ステータス。
Local host、Local	ローカル BGP スピーカーの IP アドレスとポート番号。

表 4-4　show bgp all neighbor のフィールド(続き)

フィールド	説明
Foreign host, Foreign port	ネイバーアドレスと BGP 宛先ポート番号。
Enqueued packets for retransmit:	TCP によって再送信のためにキューに格納されたパケット。
Event Timers	TCP イベントタイマー。起動およびウェイクアップのカウンタが提供されます(期限切れタイマー)。
Retrans	パケットを再送信した回数。
TimeWait	再送信タイマーが期限切れになるまで待機する時間。
AckHold	確認応答ホールドタイマー
SendWnd	伝送(送信)ウィンドウ。
KeepAlive	キープアライブパケットの数。
GiveUp	確認応答がないためにパケットがドロップされた回数。
PmtuAger	パス MTU ディスカバリタイマー。
DeadWait	デッドセグメントの有効期限タイマー。
iss:	初期パケット送信シーケンス番号。
snduna:	確認応答された最後の送信シーケンス番号。
sndnxt:	次に送信されるパケットのシーケンス番号。
sndwnd:	リモート ホストの TCP ウィンドウ サイズ。
irs:	初期パケット受信シーケンス番号。
rcvnxt:	ローカルに確認応答された最後の受信シーケンス番号。
rcvwnd:	ローカルホストの TCP ウィンドウサイズ。
delrcvwnd:	遅延受信ウィンドウ:ローカル ホストによって接続から読み取られ、ホストがリモートホストにアドバタイズした受信ウィンドウから削除されていないデータ。このフィールドの値は、フルサイズのパケットより大きくなるまで次第に増加し、それに達した時点で、rcvwnd フィールドに適用されます。
SRTT:	計算されたスムーズ ラウンドトリップ タイムアウト。
RTTO:	ラウンドトリップ タイムアウト。
RTV:	ラウンドトリップ時間の差異。
KRTT:	新しいラウンドトリップ タイムアウト(Karn アルゴリズムを使用)。このフィールドは、再送信されたパケットのラウンドトリップ時間を個別に追跡します。
minRTT:	記録された最小ラウンドトリップ タイムアウト(計算に使用される組み込み値)。
maxRTT:	記録された最大ラウンドトリップ タイムアウト。
ACK hold	ローカル ホストが追加データを伝送(ピギーバック)するために確認応答を遅らせる時間の長さ。
IP Precedence value	BGP パケットの IP プレシデンス。
Datagrams	ネイバーから受信したアップデートパケットの数。
Rcvd:	受信パケット数。

表 4-4　show bgp all neighbor のフィールド(続き)

フィールド	説明
with data	データとともに送信されたアップデートパケットの数。
total data bytes	受信データの合計量(バイト)。
Sent	送信されたアップデートパケットの数。
with data	データとともに受信したアップデート パケットの数。
total data bytes	送信データの合計量(バイト)。

show bgp cidr-only

Classless Inter-Domain Routing（CIDR）を使用したルートを表示するには、EXEC モードで **show bgp cidr-only** コマンドを使用します。

show bgp cidr-only

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、**show bgp cidr-only** コマンドの出力例をします。

```
ciscoasa# show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

表 4-5 に、各フィールドの説明を示します。

表 4-5　show bgp cidr-only のフィールド

フィールド	説明
BGP table version is 220	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス

表 4-5　show bgp cidr-only のフィールド(続き)

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp community

指定した BGP コミュニティに属するルートを表示するには、EXEC モードで **show bgp community** コマンドを使用します。

show bgp community *community-number* [**exact**]

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、特権 EXEC モードでの **show bgp community** コマンドの出力例を示します。

```
ciscoasa# show bgp community 111:12345 local-as

BGP table version is 10, local router ID is 224.0.0.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 172.16.2.2/32    10.43.222.2            0             0 222 ?
*> 10.0.0.0         10.43.222.2            0             0 222 ?
*> 10.43.0.0        10.43.222.2            0             0 222 ?
*> 10.43.44.44/32   10.43.222.2            0             0 222 ?
*  10.43.222.0/24   10.43.222.2            0             0 222 i
*> 172.17.240.0/21  10.43.222.2            0             0 222 ?
*> 192.168.212.0    10.43.222.2            0             0 222 i
*> 172.31.1.0       10.43.222.2            0             0 222 ?
```

表 4-6 に、各フィールドの説明を示します。

表 4-6　show bgp community のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス

表 4-6　show bgp community のフィールド(続き)

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp community-list

Border Gateway Protocol（BGP）コミュニティ リストで許可されたルートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp community-list** コマンドを使用します。

show bgp community-list {*community-list-number* | *community-list-name* [**exact-match**]}

構文の説明

community-list-number	1 ～ 500 の範囲の標準または拡張コミュニティ リスト番号。
community-list-name	コミュニティ リストの名前。コミュニティ リストの名前は、standard または expanded になります。
exact-match	（オプション）完全一致を持つルートだけを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する場合は、引数を指定する必要があります。**exact-match** キーワードは任意です。

例

次に、特権 EXEC モードでの **show bgp community-list** コマンドの出力例を示します。

```
ciscoasa# show bgp community-list 20

BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1             0    100      0 1800 1239 ?
*>i                 10.0.16.1             0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1             0    100      0 1800 690 568 ?
*>i                 10.0.16.1             0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1             0    100      0 1800 701 35 ?
*>i                 10.0.16.1             0    100      0 1800 701 35 ?
*                   10.92.72.24                         0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1             0    100      0 1800 690 560 ?
*>i                 10.0.16.1             0    100      0 1800 690 560 ?
*                   10.92.72.24                         0 1878 704 701 560 ?
```

```
* i10.13.0.0        10.0.22.1             0    100      0 1800 690 200 ?
*>i                 10.0.16.1             0    100      0 1800 690 200 ?
*                   10.92.72.24                         0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1             0    100      0 1800 174 ?
*>i                 10.0.16.1             0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1             0    100      0 1800 701 i
*>i                 10.0.16.1             0    100      0 1800 701 i
*                   10.92.72.24                         0 1878 704 701 i
```

表 4-7 に、各フィールドの説明を示します。

表 4-7　show bgp community-list のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

表 4-7　show bgp community-list のフィールド(続き)

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp filter-list

指定したフィルタ リストと一致するルートを表示するには、EXEC モードで **show bgp filter-list** コマンドを使用します。

show bgp filter-list *access-list-name*

構文の説明

access-list-name	自律システム パス アクセス リストの名前。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、特権 EXEC モードでの **show bgp filter-list** コマンドの出力例を示します。

```
ciscoasa# show bgp filter-list filter-list-acl

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                         0 109 108 ?
*  172.16.1.0       172.16.72.30                         0 109 108 ?
*  172.16.11.0      172.16.72.30                         0 109 108 ?
*  172.16.14.0      172.16.72.30                         0 109 108 ?
*  172.16.15.0      172.16.72.30                         0 109 108 ?
*  172.16.16.0      172.16.72.30                         0 109 108 ?
*  172.16.17.0      172.16.72.30                         0 109 108 ?
*  172.16.18.0      172.16.72.30                         0 109 108 ?
*  172.16.19.0      172.16.72.30                         0 109 108 ?
*  172.16.24.0      172.16.72.30                         0 109 108 ?
*  172.16.29.0      172.16.72.30                         0 109 108 ?
*  172.16.30.0      172.16.72.30                         0 109 108 ?
*  172.16.33.0      172.16.72.30                         0 109 108 ?
*  172.16.35.0      172.16.72.30                         0 109 108 ?
*  172.16.36.0      172.16.72.30                         0 109 108 ?
*  172.16.37.0      172.16.72.30                         0 109 108 ?
*  172.16.38.0      172.16.72.30                         0 109 108 ?
*  172.16.39.0      172.16.72.30                         0 109 108 ?
```

表 4-8 に、各フィールドの説明を示します。

表 4-8　show bgp filter-list のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp injected-paths

Border Gateway Protocol（BGP）ルーティング テーブルに注入されたすべてのパスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp injected-paths** コマンドを使用します。

show bgp injected-paths

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、EXEC モードでの **show bgp injected-paths** コマンドの出力例を示します。

```
ciscoasa# show bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                             0 ?
*> 172.17.0.0/16    10.0.0.2                             0 ?
```

表 4-9 に、各フィールドの説明を示します。

表 4-9　show bgp injected-path のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス

表 4-9　show bgp injected-path のフィールド(続き)

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv4

IP バージョン 4（IPv4）Border Gateway Protocol（BGP）ルーティング テーブル内のエントリを表示するには、特権 EXEC モードで **show bgp ipv4** コマンドを使用します。

show bgp ipv4

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、**show bgp ipv4 unicast** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv4 unicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

次に、**show bgp ipv4 multicast** コマンドの出力例を示します。

```
Router# show bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

表 4-10 に、各フィールドの説明を示します。

表 4-10　show bgp ipv4 のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6

IPv6 Border Gateway Protocol（BGP）ルーティング テーブル内のエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp ipv6** コマンドを使用します。

show bgp ipv6 unicast [***ipv6-prefix****/prefix-length*] **[longer-prefixes]** [**labels**]

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
ipv6-prefix	（オプション）IPv6 ネットワーク番号。IPv6 BGP ルーティング テーブル内の特定のネットワークを表示するために入力します。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
/prefix-length	（オプション）IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
longer-prefixes	（オプション）ルートと、より限定的なルートを表示します。
labels	（オプション）アドレス ファミリごとに、このネイバーに適用されるポリシーを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show bgp ipv6** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast

BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete


Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1             0             0  300 i
*> 10.10.20.0/24   172.16.10.1             0             0  300 i
*  10.20.10.0/24   172.16.10.1             0             0  300 i
```

次に、**show bgp ipv4 multicast** コマンドの出力例を示します。

```
Router# show bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric LocPrf Weight Path
*                   3FFE:C00:E:C::2                       0 3748 4697 1752 i
*                   3FFE:1100:0:CC00::1
                                                          0 1849 1273 1752 i
*  2001:618:3::/48  3FFE:C00:E:4::2          1            0 4554 1849 65002 i
*>                  3FFE:1100:0:CC00::1
                                                          0 1849 65002 i
*  2001:620::/35    2001:0DB8:0:F004::1
                                                          0 3320 1275 559 i
*                   3FFE:C00:E:9::2                       0 1251 1930 559 i
*                   3FFE:3600::A                          0 3462 10566 1930 559 i
*                   3FFE:700:20:1::11
                                                          0 293 1275 559 i
*                   3FFE:C00:E:4::2          1            0 4554 1849 1273 559 i
*                   3FFE:C00:E:B::2                       0 237 3748 1275 559 i
```

表 4-10 に、各フィールドの説明を示します。

表 4-11　show bgp ipv6 のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 h:テーブル エントリは履歴です。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。

表 4-11　show bgp ipv6 のフィールド(続き)

フィールド	説明
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

次に、**show bgp ipv6** コマンドの出力例を示します。ここでは、プレフィックス 3FFE:500::/24 に関する情報を示しています。

```
ciscoasa# show bgp ipv6 unicast 3FFE:500::/24

BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external

ciscoasa# show bgp ipv6 unicast

BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

show bgp ipv6 community

IPv6 Border Gateway Protocol（BGP）ルーティング テーブル内のエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp ipv6community** コマンドを使用します。

show bgp ipv6 unicast community [*community-number*] [exact-match] [local-as | no-advertise | no-export]

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
community-number	（オプション）有効な値は 1 ～ 4294967295 のコミュニティ番号、または AA:NN（自律システムのコミュニティ番号:2 バイトの番号）です。
exact-match	（オプション）完全一致を持つルートだけを表示します。
local-as	（オプション）ローカル自律システム外に送信されないルートだけを表示します（ウェルノウン コミュニティ）。
no-advertise	（オプション）ピアにアドバタイズされないルートだけを表示します（ウェルノウン コミュニティ）。
no-export	（オプション）ローカル自律システムの外部にエクスポートされていないルートだけを表示します（ウェルノウン コミュニティ）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 community** コマンドの出力は **show ip bgp community** コマンドと類似しています。

コミュニティは、**set community** ルート マップ コンフィギュレーション コマンドを使用して設定します。数値のコミュニティはウェルノウン コミュニティの前に入力する必要があります。たとえば、次の文字列は無効です。

```
ciscoasa# show ipv6 bgp unicast community local-as 111:12345
Use following strings instead:
ciscoasa# show ipv6 bgp unicast community 111:12345 local-as
```

例

次に、**show bgp ipv6 community** コマンドの出力例を示します。

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

      Network               Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64       ::                                    0 32768 i
*> 2001:0DB8:0:1:1::/80      ::                                    0 32768 ?
*> 2001:0DB8:0:2::/64        2001:0DB8:0:3::2                         0 2 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:3::2                         0 2 ?
* 2001:0DB8:0:3::1/64        2001:0DB8:0:3::2                         0 2 ?
*>                        ::                                    0 32768 ?
*> 2001:0DB8:0:4::/64        2001:0DB8:0:3::2                         0 2 ?
*> 2001:0DB8:0:5::1/64       ::                                    0 32768 ?
*> 2001:0DB8:0:6::/64        2000:0:0:3::2                         0 2 3 i
*> 2010::/64                 ::                                    0 32768 ?
*> 2020::/64                 ::                                    0 32768 ?
*> 2030::/64                 ::                                    0 32768 ?
*> 2040::/64                 ::                                    0 32768 ?
*> 2050::/64                 ::                                    0 32768 ?
```

表 4-12　show bgp ipv6 community のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 h:テーブル エントリは履歴です。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル（IGP）から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。

表 4-12　show bgp ipv6 community のフィールド(続き)

フィールド	説明
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 community-list

IPv6 Border Gateway Protocol（BGP）コミュニティ リストで許可されたルートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 community-list コマンドを使用します。

show bgp ipv6 unicast community-list {*number* | *name*} **[exact-match]**

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
number	1 ～ 199 の範囲のコミュニティ リスト番号。
name	コミュニティ リストの名前。
exact-match	（オプション）完全一致を持つルートだけを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 unicast community-list** コマンドの出力は **show ip bgp community-list** コマンドと類似しています。

例

次に、コミュニティ リスト番号 3 に対する **show ipv6 bgp community-list** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast community-list 3

BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64     2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80   2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64    ::                                     0 32768 i
*> 2001:0DB8:0:2:1::/80   ::                                     0 32768 ?
* 2001:0DB8:0:3::2/64     2001:0DB8:0:3::1                         0 1 ?
*>                      ::                                     0 32768 ?
*> 2001:0DB8:0:4::2/64    ::                                     0 32768 ?
```

```
*> 2001:0DB8:0:5::/64       2001:0DB8:0:3::1                        0 1 ?
*> 2010::/64                2001:0DB8:0:3::1                        0 1 ?
*> 2020::/64                2001:0DB8:0:3::1                        0 1 ?
*> 2030::/64                2001:0DB8:0:3::1                        0 1 ?
*> 2040::/64                2001:0DB8:0:3::1                        0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                        0 1 ?
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 4-13　show bgp ipv6 community-list のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。

表 4-13　show bgp ipv6 community-list のフィールド(続き)

フィールド	説明
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 filter-list

指定した IPv6 フィルタ リストと一致するルートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp ipv6 filter-list** コマンドを使用します。

show bgp ipv6 unicast filter-list ***access-list*-number**

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
access-list-number	IPv6 自律システム パス アクセス リストの数。1 ～ 199 の範囲の数を指定できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 filter-list** コマンドの出力は **show ip bgp filter-list** コマンドと類似しています。

例:

次に、IPv6 自律システム パス アクセス リスト番号 1 に対する **show bgp ipv6 filter-list** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast filter-list 1

BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network             Next Hop                            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64        2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:1:1::/80      2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:3::/64        2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:4::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:5::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 1 ?
*> 2001:0DB8:0:6::1/64       ::                                         32768  i
*> 2030::/64                  2001:0DB8:0:4::2                         0 1
*> 2040::/64                  2001:0DB8:0:4::2                         0 2 1 ?
*> 2050::/64                  2001:0DB8:0:4::2                         0 2 1 ?
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 4-14　show bgp ipv6 community-list のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 h:テーブル エントリは履歴です。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル（IGP）から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 inconsistent-as

送信元に一貫性のない複数の自律システムを含む IPv6 Border Gateway Protocol（BGP）ルートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 inconsistent-as を使用します。

show bgp ipv6 unicast inconsistent-as

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 unicast inconsistent-as** コマンドの出力は **show ip bgp inconsistent-as** コマンドと類似しています。

例

次に、**show bgp ipv6 inconsistent-as** コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast inconsistent-as

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                  0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                     0 1251 4270 10318 ?
*                   3FFE:3600::A                        0 3462 6175 ?
*                   3FFE:700:20:1::11                   0 293 6175 ?
```

表 4-15 この出力に表示される重要なフィールドを次に説明します。

表 4-15　show bgp ipv6 community-list のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 h:テーブル エントリは履歴です。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル（IGP）から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 neighbors

ネイバーへの IPv6 Border Gateway Protocol（BGP）接続に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 neighbors コマンドを使用します。

show bgp ipv6 unicast neighbors *[ipv6-address]* [**received-routes** | **routes** | **advertised-routes** | **paths** *regular-expression*]

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
ipv6-address	（オプション）IPv6 BGP スピーキング ネイバーのアドレス。この引数を省略した場合、すべての IPv6 ネイバーが表示されます。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
received-routes	（オプション）指定したネイバーから受信したすべてのルートを表示します。
ルート	（オプション）受信され、受け入れられるすべてのルートを表示します。これは received-routes キーワードの出力のサブセットです。
advertised-routes	（オプション）ネイバーにアドバタイズされているネットワーキング デバイスのすべてのルートを表示します。
paths *regular-expression*	（オプション）受信したパスの照合に使用される正規表現。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、show bgp ipv6 unicast neighbors コマンドの出力は show ip bgp neighbors コマンドと類似しています。

例

次に、show bgp ipv6 neighbors コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 4-16　show bgp ipv6 community-list のフィールド

フィールド	説明
BGP neighbor	BGP ネイバーの IP アドレスとその自律システム番号。ネイバーがルータと同じ自律システム内にある場合、これらの間のリンクは内部となり、そうでない場合は外部リンクと見なされます。
remote AS	ネイバーの自律システム。

表 4-16　show bgp ipv6 community-list のフィールド(続き)

フィールド	説明
internal link	このピアが内部ボーダー ゲートウェイ プロトコル(iBGP)ピアであることを示します。
BGP version	リモート ルータとの通信に使用される BGP バージョン。ネイバーのルータ ID(IP アドレス)も指定されます。
remote router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数(ドット付き 10 進表記)。
BGP state	この BGP 接続の内部ステート。
up for	ベースとなる TCP 接続が存在している時間。
Last read	BGP がこのネイバーから最後にメッセージを読み取った時間。
hold time	ピアからのメッセージ間の最大経過時間。
keepalive interval	TCP 接続が維持されていることを確認できるように、キープアライブ パケットを送信する時間間隔。
Neighbor capabilities	このネイバーからアドバタイズされ受信される BGP 機能。
Route refresh	ルート リフレッシュ機能を使用してネイバーがダイナミック ソフト リセットをサポートすることを示します。
Address family IPv6 Unicast	BGP ピアが IPv6 到達可能性情報を交換していることを示します。
Received	このピアから受信した、キープアライブを含む BGP メッセージの合計数。
通知	ピアから受信したエラー メッセージの数。
Sent	このピアに送信された、キープアライブを含む BGP メッセージの合計数。
通知	ルータがこのピアに送信したエラー メッセージの数。
advertisement runs	最小アドバタイズメント間隔の値。
For address family	後続のフィールドが参照するアドレスファミリ。
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
neighbor version	送信済みのプレフィックスおよびこのネイバーに送信する必要があるプレフィックスを追跡するためにソフトウェアによって使用された番号。
Route refresh request	このネイバーで送受信されるルート リフレッシュ要求の数。.
Community attribute(出力例になし)	neighbor send-community コマンドがこのネイバー用に設定されている場合に表示されます。
Inbound path policy(出力例になし)	インバウンド フィルタ リストまたはルート マップが設定されているかどうかを示します。

表 4-16　show bgp ipv6 community-list のフィールド(続き)

フィールド	説明
Outbound path policy（出力例になし）	アウトバウンド フィルタ リスト、ルート マップ、または抑制マップが設定されているかどうかを示します。
bgp-in（出力例になし）	IPv6 ユニキャスト アドレス ファミリのインバウンド アップデート プレフィックス フィルタ リストの名前。
aggregate（出力例になし）	IPv6 ユニキャスト アドレス ファミリのアウトバウンド アップデート プレフィックス フィルタ リストの名前。
uni-out（出力例になし）	IPv6 ユニキャスト アドレス ファミリのアウトバウンド ルート マップの名前。
accepted prefixes	受け入れられたプレフィックスの数。
Prefix advertised	アドバタイズされたプレフィックスの数。
suppressed	抑制されたプレフィックスの数。
withdrawn	取り消されたプレフィックスの数。
history paths（出力例になし）	履歴を記憶するために保持されるパス エントリの数。
Connections established	ルータが TCP 接続を確立し、2 つのピアが相互に BGP 通信を行うことに同意した回数。
dropped	良好な接続に失敗したか、ダウンした回数。
Last reset	このピアリング セッションが最後にリセットされてからの経過時間（時:分:秒形式）。
Connection state	BGP ピアの状態。
unread input bytes	処理待ちのパケットのバイト数。
Local host、Local port	ローカル ルータおよびポートのピア アドレス。
Foreign host, Foreign port	ネイバーのピア アドレス。
Event Timers	各タイマーの開始とウェイク アップの回数を表示する表。
snduna	ローカル ホストが送信したものの、確認応答を受信していない最後の送信シーケンス番号。
sndnxt	ローカル ホストが次に送信するシーケンス番号。
sndwnd	リモート ホストの TCP ウィンドウ サイズ。
irs	最初の受信シーケンス番号。
rcvnxt	ローカル ホストが確認応答した最後の受信シーケンス番号。
rcvwnd	ローカル ホストの TCP ウィンドウ サイズ。

表 4-16　show bgp ipv6 community-list のフィールド(続き)

フィールド	説明
delrecvwnd	遅延受信ウィンドウ:ローカル ホストによって接続から読み取られ、ホストがリモート ホストにアドバタイズした受信ウィンドウから削除されていないデータ。このフィールドの値は、フルサイズのパケットより大きくなるまで次第に増加し、それに達した時点で、rcvwnd フィールドに適用されます。
SRTT	計算されたスムーズ ラウンドトリップ タイムアウト(ミリ秒単位)。
RTTO	ラウンドトリップ タイムアウト(ミリ秒単位)。
RTV	ラウンドトリップ時間の差異(ミリ秒単位)。
KRTT	Karn アルゴリズムを使用した新しいラウンドトリップ タイムアウト(ミリ秒単位)。このフィールドは、再送信されたパケットのラウンドトリップ時間を個別に追跡します。
minRTT	計算に組み込み値を使用して記録された最小ラウンドトリップ タイムアウト(ミリ秒単位)。
maxRTT	記録された最大ラウンドトリップ タイムアウト(ミリ秒単位)。
ACK hold	データを「ピギーバックする」ためにローカル ホストが確認応答を遅延させる時間(ミリ秒単位)。
Flags	BGP パケットの IP プレシデンス。
Datagrams: Rcvd	ネイバーから受信したアップデート パケットの数。
with data	データとともに受信したアップデート パケットの数。
total data bytes	データのバイト総数。
Sent	送信されたアップデートパケットの数。
with data	データとともに送信されたアップデート パケットの数。
total data bytes	データのバイト総数。

次に、advertised-routes キーワードを指定した show bgp ipv6 neighbors コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                         0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                         0 3748 4697 i
```

次に、routes キーワードを指定した show bgp ipv6 neighbors コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                       0 293 7610 i
```

```
*  2001:218::/35    3FFE:700:20:1::11                    0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                    0 293 1275 3748 i
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 4-17　show bgp ipv6 neighbors advertised-routes と routes のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 h:テーブル エントリは履歴です。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル（IGP）から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

次に、paths キーワードを指定した show bgp ipv6 neighbors コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
```

次の表で、この出力に表示される重要なフィールドを説明します。

show bgp ipv6 neighbors paths のフィールド

フィールド	説明
アドレス（Address）	パスが保存される内部アドレス。
Refcount	そのパスを使用しているルートの数。
メトリック	パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。
Path	そのルートの自律システム パスと、そのルートの発信元コード。

次に、show bgp ipv6 neighbors コマンドの出力例を示します。ここでは、IPv6 アドレス 2000:0:0:4::2 の受信ルートを示しています。

```
ciscoasa# show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
Network               Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64     2000:0:0:4::2                         0 2 1 i
*> 2000:0:0:2::/64     2000:0:0:4::2                         0 2 i
*> 2000:0:0:2:1::/80   2000:0:0:4::2                         0 2 ?
*> 2000:0:0:3::/64     2000:0:0:4::2                         0 2 ?
*  2000:0:0:4::1/64    2000:0:0:4::2                         0 2 ?
```

show bgp ipv6 paths

データベース内のすべての IPv6 Border Gateway Protocol（BGP）パスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 paths コマンドを使用します。

show bgp ipv6 unicast paths *regular-expression*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
regular-expression	データベース内の受信パスの照合に使用される正規表現。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、show bgp ipv6 unicast paths コマンドの出力は show ip bgp paths コマンドと類似しています。

例

次に、show bgp ipv6 paths コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast paths
Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
アドレス（Address）	パスが保存される内部アドレス。
Refcount	そのパスを使用しているルートの数。
メトリック	パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。
Path	そのルートの自律システム パスと、そのルートの発信元コード。

show bgp ipv6 prefix-list

プレフィックス リストに一致するルートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 prefix-list コマンドを使用します。

show bgp ipv6 unicast prefix-list *name*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
name	指定したプレフィックス リスト。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

指定するプレフィックス リストは、IPv4 プレフィックス リストと同様の形式の IPv6 プレフィックス リストである必要があります。

例

```
The following is sample output from the show bgp ipv6 prefix-list command:
Router# show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 h:テーブル エントリは履歴です。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル（IGP）から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 quote-regexp

自律システム パスの正規表現に一致する IPv6 Border Gateway Protocol（BGP）ルートを引用符で囲まれた文字列として表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 quote-regexp コマンドを使用します。

show bgp ipv6 unicast quote-regexp *regular expression*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
正規表現	BGP 自律システム パスと一致させるために使用される正規表現。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、**show bgp ipv6 unicast quote-regexp** コマンドの出力は **show ip bgp quote-regexp** コマンドと類似しています。

例

次に、show bgp ipv6 quote-regexp コマンドの出力例を示します。ここでは、33 で始まるパスまたは 293 を含むパスを示しています。

```
Router# show bgp ipv6 unicast quote-regexp ^33|293
BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*  3FFE:C00:E:F::2                         0 6389 1849 293 1275
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s：テーブルエントリが抑制されます。 h：テーブル エントリは履歴です。 *：テーブルエントリが有効です。 >：テーブルエントリがそのネットワークで使用するための最良エントリです。 i：テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i：内部ゲートウェイ プロトコル（IGP）から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i：エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e：ルートは EGP で発信されました。 ?：パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 regexp

自律システム パスの正規表現に一致する IPv6 Border Gateway Protocol（BGP）ルートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 regexp コマンドを使用します。

show bgp ipv6 unicast regexp *regular-expression*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
regular-expression	BGP 自律システム パスと一致させるために使用される正規表現。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、show bgp ipv6 unicast regexp コマンドの出力は show ip bgp regexp コマンドと類似しています。

例

次に、show bgp ipv6 regexp コマンドの出力例を示します。ここでは、33 で始まるパスまたは 293 を含むパスを示しています。

```
Router# show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 h:テーブル エントリは履歴です。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル（IGP）から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 route-map

ルーティング テーブルへの登録に失敗した IPv6 Border Gateway Protocol（BGP）ルートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 route-map コマンドを使用します。

show bgp ipv6 unicast route-map *name*

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
name	照合のために指定したルート マップ。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、rmap という名前のルート マップに対する show bgp ipv6 route-map コマンドの出力例を示します。

```
Router# show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1             0    100     50 ?
*>i543::/64         2001:0DB8:101::1             0    100     50 ?
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ピリオドで区切られた 4 つのオクテットとして記述される 32 ビット数（ドット付き 10 進表記）。

フィールド	説明
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 h:テーブル エントリは履歴です。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp ipv6 summary

すべての IPv6 Border Gateway Protocol（BGP）接続のステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show bgp ipv6 summary コマンドを使用します。

show bgp ipv6 unicast summary

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

IPv6 専用である点を除いて、show bgp ipv6 unicast summary コマンドの出力は show ip bgp summary コマンドと類似しています。

例

次に、show bgp ipv6 summary コマンドの出力例を示します。

```
ciscoasa# show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor           V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2   4    200    6869     6882        0    0     0  06:25:24  Active
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
BGP device identifier	ネットワーキング デバイスの IP アドレス。
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
main routing table version	メイン ルーティング テーブルに注入された BGP データベースの最後のバージョン。

フィールド	説明
Neighbor	ネイバーの IPv6 アドレス。
V	ネイバーに通知される BGP バージョン番号。
AS	Autonomous System
MsgRcvd	ネイバーから受信された BGP メッセージ。
MsgSent	ネイバーに送信された BGP メッセージ。
TblVer	ネイバーに送信された BGP データベースの最後のバージョン。
InQ	処理を待機しているネイバーからのメッセージの数。
OutQ	ネイバーへの送信を待機しているメッセージの数。
Up/Down	BGP セッションが確立状態となったか、確立されていない場合は現在の状態になった時間の長さ。
State/ PfxRcd	BGP セッションの現在の状態/デバイスがネイバーから受信したプレフィックスの数。最大数（neighbor maximum-prefix コマンドで設定）に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルになります。 アイドル ステータスの（管理者）エントリは、接続が neighbor shutdown コマンドを使用してシャットダウンされたことを示します。

show bgp neighbors

ネイバーへの Border Gateway Protocol（BGP）接続および TCP 接続に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp neighbors** コマンドを使用します。

show bgp neighbors [**slow** | *ip-address* [**advertised-routes** | | **paths** [*reg-exp*] |**policy** [**detail**] | **received prefix-filter** | **received-routes** | **routes**]]

構文の説明

slow	（オプション）ダイナミックに設定された低速ピアに関する情報を表示します。
ip-address	（オプション）IPv4 ネイバーに関する情報を表示します。この引数を省略すると、すべてのネイバーに関する情報が表示されます。
advertised-routes	（オプション）ネイバーにアドバタイズされたすべてのルートを表示します。
paths *reg-exp*	（オプション）指定したネイバーから学習した自律システムパスを表示します。オプションの正規表現を使用して、出力をフィルタ処理できます。
ポリシー	（オプション）アドレス ファミリごとに、このネイバーに適用されるポリシーを表示します。
detail	（オプション）ルート マップ、プレフィックス リスト、コミュニティ リスト、アクセス コントロール リスト（ACL）、自律システム パス フィルタ リストなどの詳細なポリシー情報を表示します。
received prefix-filter	（オプション）指定したネイバーから送信されたプレフィックス リスト（アウトバウンド ルート フィルタ（ORF））を表示します。
received-routes	（オプション）指定したネイバーから受信したすべてのルートを表示します。
routes	（オプション）受信され、受け入れられるすべてのルートを表示します。このキーワードが入力されたときに表示される出力は、**received-routes** キーワードによって表示される出力のサブセットです。

コマンド デフォルト

このコマンドの出力には、すべてのネイバーの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ネイバー セッションの BGP および TCP 接続情報を表示するには、**show bgp neighbors** コマンドを使用します。BGP の場合、これには詳細なネイバー属性、機能、パス、およびプレフィックス情報が含まれています。TCP の場合、これには BGP ネイバー セッション確立およびメンテナンスに関連した統計が含まれています。

アドバタイズされ、取り消されたプレフィックスの数に基づいて、プレフィックス アクティビティが表示されます。ポリシー拒否には、アドバタイズされたものの、その後、出力に表示されている機能または属性に基づいて無視されたルートの数が表示されます。

シスコが採用している 4 バイト自律システム番号では、自律システム番号の正規表現のマッチングおよび出力表示のデフォルトの形式として asplain（たとえば、65538）を使用していますが、RFC 5396 で定義されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドに続けて、**clear bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。

例

出力例は、**show bgp neighbors** コマンドで使用できるさまざまなキーワードによって異なります。以降のセクションでは、さまざまなキーワードの使用例を示します。

show bgp neighbors：例

次に、10.108.50.2 の BGP ネイバーの出力例を示します。このネイバーは、内部 BGP（iBGP）ピアです。ルート更新とグレースフル リスタート機能をサポートしています。

```
ciscoasa# show bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
```

```
  1 update-group member
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

次の表で、この出力に表示される重要なフィールドを説明します。アスタリスク文字(*)の後ろにあるフィールドは、カウンタが非ゼロ値の場合だけ表示されます。

表 4-10 に、各フィールドの説明を示します。

表 4-18　show bgp ipv4 のフィールド

フィールド	説明
BGP neighbor	BGP ネイバーの IP アドレスとその自律システム番号。
remote AS	ネイバーの自律システム番号。

表 4-18　show bgp ipv4 のフィールド(続き)

フィールド	説明
local AS 300 no-prepend(出力には表示されない)	ローカルの自律システム番号が受信された外部ルートの先頭に付加されていないことを確認します。この出力は、自律システムを移行しているときのローカル自律システムの非表示をサポートします。
internal link	iBGP ネイバーの場合「internal link」と表示されます。外部 BGP(eBGP)ネイバーの場合は「external link」と表示されます。
BGP version	リモート ルータとの通信に使用される BGP バージョン。
remote router ID	ネイバーの IP アドレス。
BGP state	セッション ネゴシエーションの有限状態マシン(FSM)ステージ。
up for	ベースとなる TCP 接続が存在している時間(hhmmss 形式)。
Last read	BGP がこのネイバーから最後にメッセージを受信してからの時間(hhmmss 形式)。
last write	BGP がこのネイバーに最後にメッセージを送信してからの時間(hhmmss 形式)。
hold time	BGP がメッセージを受信せずにこのネイバーとセッションを維持した時間(秒数)。
keepalive interval	キープアライブ メッセージがこのネイバーに転送される間隔(秒数)。
Neighbor capabilities	このネイバーからアドバタイズされ受信される BGP 機能。2 つのルータ間で機能が正常に交換されている場合、「advertised and received」が表示されます。
Route Refresh	ルート リフレッシュ機能のステータス。
Graceful Restart Capability	グレースフル リスタート機能のステータス。
Address family IPv4 Unicast	このネイバーの IP Version 4 ユニキャスト固有プロパティ。
Message statistics	メッセージ タイプごとにまとめられた統計。
InQ depth is	入力キュー内のメッセージ数。
OutQ depth is	出力キュー内のメッセージ数。
Sent	送信されたメッセージの合計数。
Received	受信されたメッセージの合計数。
Opens	送受信されたオープンメッセージ数。
通知	送受信された通知(エラー)メッセージ数。
Updates	送受信されたアップデートメッセージ数。
Keepalives	送受信されたキープアライブメッセージ数。
Route Refresh	送受信されたルートリフレッシュ要求メッセージ数。
Total	送受信されたメッセージの合計数。
Default minimum time between...	アドバタイズメント送信の間の時間(秒数)。
For address family:	後続のフィールドが参照するアドレスファミリ。

表 4-18　show bgp ipv4 のフィールド(続き)

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
neighbor version	送信済みのプレフィックスおよび送信する必要があるプレフィックスを追跡するためにソフトウェアによって使用された番号。
update-group	このアドレス ファミリのアップデート グループ メンバーの数。
Prefix activity	このアドレスファミリのプレフィックス統計。
Prefixes current	このアドレス ファミリに対して受け入れられるプレフィックス数。
Prefixes total	受信されたプレフィックスの合計数。
Implicit Withdraw	プレフィックスが取り消されて再アドバタイズされた回数。
Explicit Withdraw	フィージブルでなくなったため、プレフィックスが取り消された回数。
Used as bestpath	最適パスとしてインストールされた受信プレフィックス数。
Used as multipath	マルチパスとしてインストールされた受信プレフィックス数。
* Saved（ソフト再構成）	ソフト再構成をサポートするネイバーで実行されたソフトリセットの数。このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。
* History paths	このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。
* Invalid paths	無効なパスの数。このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。
Local Policy Denied Prefixes	ローカルポリシー設定が原因で拒否されたプレフィックス。カウンタは、インバウンドおよびアウトバウンドのポリシー拒否ごとに更新されます。この見出しの下のフィールドは、カウンタの値がゼロ以外である場合にだけ表示されます。
* route-map	インバウンドおよびアウトバウンドのルートマップポリシー拒否を表示します。
* filter-list	インバウンドおよびアウトバウンドのフィルタリストポリシー拒否を表示します。
* prefix-list	インバウンドおよびアウトバウンドのプレフィックスリスト ポリシー拒否を表示します。
* AS_PATH too long	アウトバウンドの AS パス長ポリシー拒否を表示します。
* AS_PATH loop	アウトバウンドの AS パス ループ ポリシー拒否を表示します。
* AS_PATH confed info	アウトバウンド コンフェデレーション ポリシー拒否を表示します。
* AS_PATH contains AS 0	自律システム（AS）0 のアウトバウンド拒否を表示します。
* NEXT_HOP Martian	アウトバウンドの Martian 拒否を表示します。
* NEXT_HOP non-local	アウトバウンドの非ローカル ネクスト ホップ拒否を表示します。
* NEXT_HOP is us	アウトバウンドのネクストホップ自身の拒否を表示します。
* CLUSTER_LIST loop	アウトバウンドのクラスタリスト ループ拒否を表示します。

表 4-18　show bgp ipv4 のフィールド(続き)

フィールド	説明
* ORIGINATOR loop	ローカルで発信されたルートのアウトバウンド拒否を表示します。
* unsuppress-map	抑制マップによるインバウンド拒否を表示します。
* advertise-map	アドバタイズ マップによるインバウンド拒否を表示します。
* Well-known Community	ウェルノウン コミュニティのインバウンド拒否を表示します。
* SOO loop	site-of-origin によるインバウンド拒否を表示します。
* Bestpath from this peer	最適パスがローカル ルータから提供されたことによるインバウンド拒否を表示します。
* Suppressed due to dampening	ネイバーまたはリンクがダンプニング状態であることによるインバウンド拒否を表示します。
* Bestpath from iBGP peer	最適パスが iBGP ネイバーから提供されたことによるインバウンド拒否を表示します。
* Incorrect RIB for CE	CE ルータの RIB エラーによるインバウンド拒否を表示します。
* BGP distribute-list	配布リストによるインバウンド拒否を表示します。
Number of NLRIs...	アップデート内のネットワーク層到達可能性属性の数。
Connections established	TCP および BGP 接続が正常に確立した回数。
dropped	有効セッションに障害が発生したか停止した回数。
Last reset	このピアリング セッションが最後にリセットされてからの時間。リセットがこの行に表示された理由。
External BGP neighbor may be... (出力には表示されない)	BGP TTL セキュリティ チェックがイネーブルであることを示します。ローカルピアとリモートピアをまたぐことができるホップの最大数がこの行に表示されます。
Connection state	BGP ピアの接続ステータス。
Connection is ECN Disabled	明示的輻輳通知のステータス(イネーブルまたはディセーブル)。
Local host: 10.108.50.1, Local port: 179	ローカル BGP スピーカーの IP アドレス。BGP ポート番号 179。
Foreign host: 10.108.50.2, Foreign port: 42698	ネイバーアドレスと BGP 宛先ポート番号。
Enqueued packets for retransmit:	TCP によって再送信のためにキューに格納されたパケット。
Event Timers	TCP イベントタイマー。起動およびウェイクアップのカウンタが提供されます(期限切れタイマー)。
Retrans	パケットを再送信した回数。
TimeWait	再送信タイマーが期限切れになるまで待機する時間。

表 4-18　show bgp ipv4 のフィールド(続き)

フィールド	説明
AckHold	確認応答ホールドタイマー
SendWnd	伝送(送信)ウィンドウ。
KeepAlive	キープアライブパケットの数。
GiveUp	確認応答がないためにパケットがドロップされた回数。
PmtuAger	パス MTU ディスカバリ タイマー。
DeadWait	デッドセグメントの有効期限タイマー。
iss:	初期パケット送信シーケンス番号。
snduna	確認応答されなかった最後の送信シーケンス番号。
sndnxt:	次に送信されるパケットのシーケンス番号。
sndwnd:	リモートネイバーの TCP ウィンドウ サイズ。
irs:	初期パケット受信シーケンス番号。
rcvnxt:	ローカルに確認応答された最後の受信シーケンス番号。
rcvwnd:	ローカルホストの TCP ウィンドウサイズ。
delrcvwnd:	遅延受信ウィンドウ:ローカル ホストによって接続から読み取られ、ホストがリモートホストにアドバタイズした受信ウィンドウから削除されていないデータ。このフィールドの値は、フルサイズのパケットより大きくなるまで次第に増加し、それに達した時点で、rcvwnd フィールドに適用されます。
SRTT:	計算されたスムーズ ラウンドトリップ タイムアウト。
RTTO:	ラウンドトリップ タイムアウト。
RTV:	ラウンドトリップ時間の差異。
KRTT:	新しいラウンドトリップ タイムアウト(Karn アルゴリズムを使用)。このフィールドは、再送信されたパケットのラウンドトリップ時間を個別に追跡します。
minRTT:	記録された最小ラウンドトリップ タイムアウト(計算に使用される組み込み値)。
maxRTT:	記録された最大ラウンドトリップ タイムアウト。
ACK hold:	ローカル ホストが追加データを伝送(ピギーバック)するために確認応答を遅らせる時間の長さ。
IP Precedence value:	BGP パケットの IP プレシデンス。
Datagrams	ネイバーから受信したアップデートパケットの数。
Rcvd:	受信パケット数。
with data	データとともに送信されたアップデートパケットの数。
total data bytes	受信データの合計量(バイト)。
Sent	送信されたアップデートパケットの数。
Second Congestion	輻輳による再送信に要した秒数。
Datagrams: Rcvd	ネイバーから受信したアップデートパケットの数。
out of order:	シーケンスを外れて受信したパケットの数。

表 4-18　show bgp ipv4 のフィールド(続き)

フィールド	説明
with data	データとともに受信したアップデート パケットの数。
Last reset	このピアリング セッションが最後にリセットされてからの経過時間。
unread input bytes	処理待ちのパケットのバイト数。
retransmit	再送信されたパケット数。
fastretransmit	再送信タイマーが期限切れになる前に、順序が不正なセグメントのために再送信された重複する確認応答の数。
partialack	部分的な確認応答(後続の確認応答がない、またはそれ以前の送信)のために再送信された回数。

show bgp neighbors advertised-routes:例

次に、172.16.232.178 ネイバーのみにアドバタイズされたルートを表示する例を示します。

```
ciscoasa# show bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

表 4-19 に、各フィールドの説明を示します。

表 4-19　show bgp neighbors advertised routes のフィールド

フィールド	説明
BGP table version	テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。
local router ID	ルータの IP アドレス
Status codes	テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。 s:テーブルエントリが抑制されます。 *:テーブルエントリが有効です。 >:テーブルエントリがそのネットワークで使用するための最良エントリです。 i:テーブルエントリが内部 BGP(iBGP)セッションを経由して学習されます。
Origin codes	エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。 i:内部ゲートウェイ プロトコル(IGP)から発信され、**network** ルータ コンフィギュレーション コマンドを使用してアドバタイズされたエントリ。 e:エクステリア ゲートウェイ プロトコル(EGP)から発信されたエントリ。 ?:パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。
Network	エントリが表すネットワークのインターネット アドレス。

表 4-19　show bgp neighbors advertised routes のフィールド（続き）

フィールド	説明
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、アクセス サーバにこのネットワークへの非 BGP ルートがあることを示します。
Metric	表示されている場合は相互自律システム メトリック。
LocPrf	**set local-preference** ルート マップ コンフィギュレーション コマンドで設定されたローカル プリファレンス値。デフォルト値は 100 です。
Weight	自律システムフィルタを介して設定されたルートの重み。
Path	宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。パスの終わりは、パスの発信元コードです。 i:エントリは IGP で発信され、**network** ルータ コンフィギュレーション コマンドでアドバタイズされました。 e:ルートは EGP で発信されました。 ?:パスの発信元が明確ではありません。通常、これは、IGP から BGP に再配布されたパスです。

show bgp neighbors paths：例

次に、**paths** キーワードを指定した **show bgp neighbors** コマンドの出力例を示します。

```
ciscoasa# show bgp neighbors 172.29.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

表 4-20 に、各フィールドの説明を示します。

表 4-20　show bgp neighbors paths のフィールド

フィールド	説明
アドレス（Address）	パスが保存される内部アドレス。
Refcount	そのパスを使用しているルートの数。
メトリック	パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。
パス	そのルートの自律システム パスと、そのルートの発信元コード。

show bgp neighbors received prefix-filter：例

次の例は、10.0.0.0 ネットワークのすべてのルートをフィルタリングするプレフィックス リストが 192.168.20.72 ネイバーから受信されたことを示しています。

```
ciscoasa# show bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

表 4-21 に、各フィールドの説明を示します。

表 4-21　show bgp neighbors received prefix filter のフィールド

フィールド	説明
Address family	プレフィックスフィルタが受信されるアドレスファミリモード。
ip prefix-list	指定したネイバーから送信されたプレフィックスリスト。

show bgp neighbors policy：例

次に、192.168.1.2 にあるネイバーに適用されたポリシーの出力例を示します。ネイバー デバイスで設定されたポリシーが表示されます。

```
ciscoasa# show bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

show bgp neighbors：例

次に、**show bgp neighbors** コマンドの出力例を示します。ここでは、BGP TCP パス最大伝送ユニット（MTU）ディスカバリが 172.16.1.2 にある BGP ネイバーに対して有効になっていることを確認しています。

```
ciscoasa# show bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

次に、**show bgp neighbors** コマンドの出力の一部を示します。ここでは、192.168.3.2 にある外部 BGP ピアに対する BGP グレースフル リスタート機能のステータスを確認しています。グレースフル リスタートは、この BGP ピアに対してディセーブルであると示されています。

```
ciscoasa# show bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

show bgp paths

データベース内のすべての BGP パスを表示するには、EXEC モードで **show bgp paths** コマンドを使用します。

show bgp paths

Cisco 10000 シリーズ ルータ

show bgp paths *regexp*

構文の説明

regexp	BGP 自律システム パスと一致する正規表現。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、特権 EXEC モードでの **show bgp paths** コマンドの出力例を示します。

```
ciscoasa# show bgp paths

Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

表 4-22 に、各フィールドの説明を示します。

表 4-22　show bgp paths のフィールド

フィールド	説明
アドレス（Address）	パスが保存される内部アドレス。
Hash	パスが格納されているハッシュ バケット。
Refcount	そのパスを使用しているルートの数。

表 4-22　show bgp paths のフィールド(続き)

フィールド	説明
メトリック	パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。
Path	そのルートの自律システム パスと、そのルートの発信元コード。

show bgp policy-list

設定されたポリシー リストとポリシー リスト エントリに関する情報を表示するには、ユーザ EXEC モードで **show bgp policy-list** コマンドを使用します。

show bgp policy-list [*policy-list-name*]

構文の説明

policy-list-name	（オプション）この引数を使用して指定したポリシー リストに関する情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、**show bgp policy-list** コマンドの出力例を示します。このコマンドの出力には、ポリシー リスト名と設定された match 句が表示されます。次の出力例は、表示される出力に類似しています。

```
ciscoasa# show bgp policy-list

policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

show bgp prefix-list

プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp prefix-list** コマンドを使用します。

show bgp prefix-list [**detail** | **summary**][*prefix-list-name* [**seq** *sequence-number* | *network/length* [**longer**| **first-match**]]]

構文の説明

detail	**summary**	(オプション)すべてのプレフィックス リストに関する詳細情報または要約情報を表示します。
first-match	(オプション) 指定した *network/length* と一致する、指定したプレフィックス リストの最初のエントリを表示します。
longer	(オプション)指定した *network/length と一致するか、またはより限定的な、プレフィックス リストのすべてのエントリを表示します。*
network/length	(オプション)このネットワーク アドレスおよびネットマスク長(ビット単位)を使用する、指定したプレフィックス リストのすべてのエントリを表示します。
prefix-list-name	(オプション)特定のプレフィックス リストのエントリを表示します。
seq *sequence-number*	(オプション)指定したプレフィックス リストに指定したシーケンス番号があるプレフィックス リスト エントリだけを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、**show bgp prefix-list** コマンドの出力例を示します。ここでは、test という名前のプレフィックス リストの詳細を示しています。

```
ciscoasa# show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

show bgp regexp

自律システム パスの正規表現と一致するルートを表示するには、EXEC モードで **show bgp regexp** コマンドを使用します。

show bgp regexp *regexp*

構文の説明

regexp	BGP 自律システム パスと一致する正規表現。 自律システムの番号形式の詳細については、**router bgp** コマンドの説明を参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

シスコが採用している 4 バイト自律システム番号では、自律システム番号の正規表現のマッチングおよび出力表示のデフォルトの形式として asplain（たとえば、65538）を使用していますが、RFC 5396 で定義されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドに続けて、**clear bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。

円滑に移行するには、4 バイト自律システム番号を使用して指定されている自律システム内にあるすべての BGP スピーカーで、4 バイト自律システム番号をサポートするようアップグレードすることを推奨します。

例

次に、特権 EXEC モードでの **show bgp regexp** コマンドの出力例を示します。

```
Router# show bgp regexp 108$

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
```

```
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

bgp asnotation dot コマンドを設定すると、4 バイト自律システム パスの正規表現一致形式が asdot 表記法の形式に変更されます。4 バイト自律システム番号は、asplain 形式または asdot 形式のいずれかを使用して、正規表現で設定できますが、現在のデフォルト形式を使用して設定された 4 バイト自律システム番号だけがマッチングされます。1 つ目の例では、**show bgp regexp** コマンドは、asplain 形式で表された 4 バイト自律システム番号を使用して設定されています。現在のデフォルト形式は asdot 形式なのでマッチングは失敗し、何も出力されません。asdot 形式を使用した 2 番目の例では、マッチングは成功し、4 バイトの自律システム パスに関する情報が asdot 表記法を使って表示されます。

(注) asdot 表記法では、シスコの正規表現で特殊文字であるピリオドを使用します。特殊な意味を削除するには、ピリオドの前にバックスラッシュを使用します。

```
Router# show bgp regexp ^65536$

Router# show bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

次に、**bgp asnotation dot** コマンドを入力した後の **show bgp regexp** コマンドの出力例を示します。ここでは、4 バイト自律システム番号を表示しています。

(注) asdot 表記法では、シスコの正規表現で特殊文字であるピリオドを使用します。特殊な意味を削除するには、ピリオドの前にバックスラッシュを使用します。

```
Router# show bgp regexp ^1\.14$

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.14   i
```

show bgp replication

Border Gateway Protocol（BGP）アップデート グループのアップデート複製統計情報を表示するには、EXEC モードで **show bgp replication** コマンドを使用します。

show bgp replication [*index-group* | *ip-address*]

構文の説明

index-group	（オプション）アップデート グループのアップデート複製統計情報を対応するインデックス番号とともに表示します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。
ip-address	（オプション）このネイバーのアップデート複製統計情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの出力には、BGP アップデート グループ複製統計情報が表示されます。

アウトバウンド ポリシーが変更された場合、ルータは、3 分間のタイマー期限が切れた後で、アウトバウンド ソフト リセットをトリガーすることにより、自動的にアップデート グループ メンバーシップを再計算し、変更を適用します。この動作は、ネットワーク オペレータがミスを犯した場合に、コンフィギュレーションを変更する時間を与えるように設計されています。タイマー期限が切れる前に、アウトバウンド ソフト リセットを手動で有効にするには、**clearbgp** *ip-address* **soft out** コマンドを入力します。

例

次の **show bgp replication** コマンドの出力例には、すべてのネイバーのアップデート グループの複製情報が表示されます。

```
ciscoasa# show bgp replication

BGP Total Messages Formatted/Enqueued : 0/0

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
         2 internal        2        10.4.9.5        0        0      0      0
The following sample output from the show bgp replication command shows update-group
statistics for the 10.4.9.5 neighbor:
Router# show bgp replication 10.4.9.5
```

```
  Index      Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
      2 internal        2        10.4.9.5        0        0      0      0
```

表 4-23 に、各フィールドの説明を示します。

表 4-23　show bgp replication のフィールド

フィールド	説明
Index	アップデート グループのインデックス番号。
タイプ	ピアのタイプ（内部または外部）。
Members	ダイナミック アップデート ピア グループ内のメンバーの数。
Leader	ダイナミック アップデート ピア グループの最初のメンバー。

show bgp rib-failure

ルーティング情報ベース（RIB）テーブルへの登録に失敗した Border Gateway Protocol（BGP）ルートを表示するには、特権 EXEC モードで **show bgp rib-failure** コマンドを使用します。

show bgp rib-failure

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、**show bgp rib-failure** コマンドの出力例を示します。

```
ciscoasa# show bgp rib-failure

Network          Next Hop                  RIB-failure   RIB-NH Matches
10.1.15.0/24     10.1.35.5          Higher admin distance             n/a
10.1.16.0/24     10.1.15.1          Higher admin distance             n/a
```

表 4-24 に、各フィールドの説明を示します。

表 4-24　show bgp rib-failure のフィールド

フィールド	説明
ネットワーク	ネットワーク エンティティの IP アドレス。
Next Hop	パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、ルータにこのネットワークへの非 BGP ルートがあることを示します。
RIB-failure	RIB 失敗の原因。アドミニストレイティブ ディスタンスが高いということは、スタティック ルートなど優れた（低い）アドミニストレーティブ ディスタンスを持つルートが IP ルーティング テーブルにすでにあることを意味します。

表 4-24　show bgp rib-failure のフィールド(続き)

フィールド	説明
RIB-NH Matches	より高いアドミニストレイティブ ディスタンスが RIB-failure 列に表示され、使用されるアドレス ファミリに対して **bgp suppress-inactive** が設定されている場合にだけ適用されるルート ステータス。次の 3 種類があります。 • [Yes]：RIB のルートに BGP ルートと同じネクスト ホップがあるか、またはネクスト ホップが BGP ネクスト ホップと同じ隣接に再帰することを意味します。 • [No]：RIB のネクスト ホップが BGP ルートのネクスト ホップとは別に再帰することを意味します。 • [n/a]：使用されるアドレス ファミリに対して **bgp suppress-inactive** が設定されないことを意味します。

show bgp summary

すべての Border Gateway Protocol（BGP）接続のステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp summary** コマンドを使用します。

show bgp summary

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

show bgp summary コマンドは、BGP ネイバーへのすべての接続について BGP パス、プレフィックス、および属性情報を表示するために使用します。

プレフィックスは、IP アドレスとネットワーク マスクです。これはネットワーク全体、ネットワークのサブセット、または単一のホスト ルートを表すことができます。パスは、所定の宛先へのルートです。デフォルトでは、BGP は宛先ごとに 1 つのパスだけをインストールします。マルチパス ルートが設定されている場合、BGP は各マルチパス ルートにパス エントリをインストールし、1 つのマルチパス ルートにのみ最適パスとマークされます。

BGP 属性とキャッシュ エントリは個別にも組み合わせても表示され、これは最適パス選択プロセスに影響を与えます。この出力のフィールドは、関連する BGP 機能が設定されているか、または属性が受信されたときに表示されます。メモリ使用量はバイト単位で表示されます。

シスコが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドに続けて、**clear bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。

例

次に、特権 EXEC モードでの **show bgp summary** コマンドの出力例を示します。

```
Router# show bgp summary

BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
```

```
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

表 4-25 に、各フィールドの説明を示します。

表 4-25　show bgp summary のフィールド

フィールド	説明
BGP router identifier	優先度とアベイラビリティの順序で、**bgp router-id** コマンドによって指定されたルータ ID、ループバック アドレス、または最上位 IP アドレス。
BGP table version	BGP データベースの内部バージョン番号。
main routing table version	メイン ルーティング テーブルに注入された BGP データベースの最後のバージョン。
...network entries	BGP データベースの一意のプレフィックス エントリの数。
...using ... bytes of memory	同じ行のパス、プレフィックス、または属性のエントリのために消費されているメモリ量(バイト単位)。
...path entries using	BGP データベースのパス エントリの数。単一のパス エントリだけが特定の宛先にインストールされます。マルチパス ルートが設定されている場合、マルチパス ルートごとにパス エントリがインストールされます。
...multipath network entries using	特定の宛先にインストールされているマルチパス エントリの数。
* ...BGP path/bestpath attribute entries using	パスが最適パスとして選択されている一意の BGP 属性の組み合わせの数。
* ...BGP rrinfo entries using	ORIGINATOR 属性と CLUSTER_LIST 属性の一意の組み合わせの数。
...BGP AS-PATH entries using	一意の AS_PATH エントリの数。
...BGP community entries using	BGP コミュニティ属性の一意の組み合わせの数。
*...BGP extended community entries using	拡張コミュニティ属性の一意の組み合わせの数。

表 4-25　show bgp summary のフィールド(続き)

フィールド	説明
BGP route-map cache entries using	BGP ルート マップの match 句と set 句の組み合わせの数。値が 0 の場合、ルート キャッシュが空であることを示します。
...BGP filter-list cache entries using	AS パス アクセス リストの permit ステートメントまたは deny ステートメントに一致するフィルタ リスト エントリの数。値が 0 の場合、フィルタ リスト キャッシュが空であることを示します。
BGP advertise-bit cache entries using	(Cisco IOS Release 12.4(11)T 以降のリリースだけ)アドバタイズされたビット フィールド エントリの数および関連するメモリ使用量。ビット フィールド エントリは、プレフィックスがピアにアドバタイズされるときに生成される情報(1 ビット)を表します。アドバタイズされたビット キャッシュは、必要に応じてダイナミックに作成されます。
...received paths for inbound soft reconfiguration	インバウンド ソフト再構成のために受信され保存されるパスの数。
BGP using...	BGP プロセスによって使用されるメモリの総量(バイト単位)。
Dampening enabled...	BGP ダンプニングがイネーブルであることを示します。この行には、累積ペナルティを伝送するパスの数およびダンプニングされたパスの数が表示されます。
BGP activity...	パスまたはプレフィックスに対してメモリが割り当てられたか、または解放された回数を表示します。
Neighbor	ネイバーの IP アドレス。
V	ネイバーに通知される BGP バージョン番号。
AS	自律システム(AS)番号。
MsgRcvd	ネイバーから受信されたメッセージ数。
MsgSent	ネイバーに送信されたメッセージ数。
TblVer	ネイバーに送信された BGP データベースの最終バージョン。
InQ	ネイバーで処理するためにキューに格納されたメッセージ数。
OutQ	ネイバーに送信するために、キューに格納されたメッセージ数。
Up/Down	BGP セッションが確立状態となったか、確立状態ではない場合は現在の状態になった時間の長さ。
State/PfxRcd	BGP セッションの現在の状態と、ネイバーまたはピア グループから受信されたプレフィックスの数。最大数(**neighbor maximum-prefix** コマンドで設定)に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルに設定されます。 アイドル ステータスの(管理者)エントリは、**neighbor shutdown** コマンドを使用して接続がシャットダウンされたことを示します。

show bgp summary コマンドの次の出力は、BGP ネイバー 192.168.3.2 がダイナミックに作成され、この受信範囲グループであるグループ 192 のメンバーであることを示します。この出力は、IP プレフィックス範囲 192.168.0.0/16 がグループ 192 という名前の受信範囲グループに定義されることも示します。Cisco IOS リリース 12.2(33)SXH 以降のリリースでは、BGP ダイナミック ネイバー機能により、ピア グループ(受信範囲グループ)に関連付けられたサブネット範囲を使用して BGP ネイバー ピアのダイナミックな作成をサポートする機能が追加されました。

```
ciscoasa# show bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

show bgp summary コマンドの次の出力は、4 バイトの異なる自律システム番号（65536 および 65550）の 2 つの BGP ネイバー（192.168.1.2 および 192.168.3.2）を示しています。ローカルな自律システム 65538 は、4 バイト自律システム番号でもあり、その番号はデフォルトの asplain 形式で表示されます。

```
Router# show bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15      0
```

show bgp summary コマンドの次の出力は同じ 2 つの BGP ネイバーを示していますが、4 バイト自律システム番号は asdot 表記法の形式で表示されます。表示形式を変更するには、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを設定する必要があります。

```
Router# show bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4         1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4        1.14       6       6        1    0    0 00:01:24      0
```

次に、**show bgp summary slow** コマンドの出力例を示します。

```
ciscoasa> show bgp summary slow
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 37, main routing table version 37
36 network entries using 4608 bytes of memory
36 path entries using 1872 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6700 total bytes of memory
BGP activity 46/0 prefixes, 48/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
6.6.6.6 4 100 11 10 1 0 0 00:44:20 0
```

show bgp system-config

ユーザ コンテキストでシステム コンテキストの bgp の実行コンフィギュレーションを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show bgp system-config** コマンドを使用します。

show bgp system-config

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC、ユーザ EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、引数またはキーワードを指定せずにユーザ コンテキストでだけ使用できます。このコマンドは、システム コンテキストによってユーザ コンテキストに対して適用される実行コンフィギュレーションを確認する場合に役立つことがあります。

例

次の出力例は、**show bgp system-config** コマンドをユーザ EXEC モードで入力すると表示される出力に類似しています。

```
ciscoasa/c1(config)# show bgp system-config
router bgp 1
 bgp log-neighbor-changes
 no bgp always-compare-med
 no bgp asnotation dot
 no bgp bestpath med
 no bgp bestpath compare-routerid
 bgp default local-preference 100
 no bgp deterministic-med
 bgp enforce-first-as
 bgp maxas-limit 0
 bgp transport path-mtu-discovery
 timers bgp 60 180 0
 address-family ipv4 unicast
  bgp scan-time 0
  bgp nexthop trigger enable
  bgp nexthop trigger delay 5
 exit-address-family
```

show blocks

パケット バッファの使用状況を表示するには、特権 EXEC モードで **show blocks** コマンドを使用します。

show blocks [{**address** *hex* | **all** | **assigned** | **free** | **old** | **pool** *size* [**summary**]} [**diagnostics** | **dump** | **header** | **packet**] | **queue history** | [**exhaustion snapshot** | **history** [**list**] [*1-MAX_NUM_SNAPSHOT* | *index*] [**detail**]]

構文の説明

address *hex*	(任意)このアドレスに対応するブロックを 16 進数形式で表示します。
all	(任意)すべてのブロックを表示します。
assigned	(任意)割り当て済みでアプリケーションによって使用されているブロックを表示します。
detail	(任意)一意のキュー タイプごとに最初のブロックの一部(128 バイト)を表示します。
dump	(任意)ヘッダーとパケットの情報を含め、ブロックの内容全体を表示します。dump と packet の相違点は、dump の場合、ヘッダーとパケットに関する追加情報が含まれることです。
診断	(任意)ブロックの診断を表示します。
exhaustion snapshot	(オプション)取得されたスナップショットの最後の x 番号(x は現時点では 10)および最後のスナップショットのタイムスタンプを出力します。スナップショットが取得された後、5 分以上経過しないと別のスナップショットは取得されません。
free	(任意)使用可能なブロックを表示します。
header	(任意)ブロックのヘッダーを表示します。
history *1-MAX_NUM_SNAPSHOT* **history** *index* **history list**	**history** オプションは、最近のスナップショットと履歴内のすべてのスナップショットを表示します。 **history list** オプションは、履歴内のスナップショットの要約を表示します。 **history** *index* オプションは、履歴内のスナップショットのインデックスを表示します。 **history** *1-MAX_NUM_SNAPSHOT* オプションは、履歴内の 1 つのスナップショットだけを表示します。
old	(任意)1 分よりも前に割り当てられたブロックを表示します。
パケット	(任意)ブロックのヘッダーおよびパケットの内容を表示します。
pool *size*	(任意)特定のサイズのブロックを表示します。
queue history	(任意)ASA がブロックを使い果たしたときに、ブロックが割り当てられる位置を表示します。プール内のブロックが割り当てられることはありますが、ブロックがキューに割り当てられることはありません。この場合は、ブロックを割り当てたコードのアドレスが割り当て場所になります。

summary	(任意)ブロックの使用状況に関する詳細情報を表示します。この情報は、このクラスにブロックを割り当てたアプリケーションのプログラム アドレス、このクラスのブロックを解放したアプリケーションのプログラム アドレス、およびこのクラスの有効なブロックが属しているキューを基準としてソートされています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	**pool summary** オプションが追加されました。
8.0(2)	dupb ブロックは、4 バイト ブロックではなく長さが 0 のブロックを使用するようになりました。0 バイト ブロック用の 1 行が追加されました。
9.1(5)	**exhaustion snapshot**、**history** list、**history** *index*、**history** *1-MAX_NUM_SNAPSHOT* の各オプションが追加されました。

使用上のガイドライン

show blocks コマンドは、ASA が過負荷になっているかどうかを判断する場合に役立ちます。このコマンドは、事前割り当て済みのシステム バッファの使用状況を表示します。トラフィックが ASA 経由で伝送されている限り、メモリがいっぱいになっている状態は問題にはなりません。**show conn** コマンドを使用すると、トラフィックが伝送されているかどうかを確認できます。トラフィックが伝送されておらず、かつメモリがいっぱいになっている場合は、問題がある可能性があります。

この情報は、SNMP を使用して表示することもできます。

セキュリティ コンテキスト内で表示される情報には、使用中のブロック、およびブロック使用状況の高基準値に関する、システム全体の情報およびコンテキスト固有の情報が含まれます。

出力の説明については、「例」を参照してください。

例

次に、シングル モードでの **show blocks** コマンドの出力例を示します。

```
ciscoasa# show blocks
  SIZE    MAX    LOW    CNT
     0    100     99    100
     4   1600   1598   1599
    80    400    398    399
   256   3600   3540   3542
```

```
  1550    4716    3177    3184
 16384      10      10      10
  2048    1000    1000    1000
```

表 4-26 に、各フィールドの説明を示します。

表 4-26　show blocks のフィールド

フィールド	説明
SIZE	ブロック プールのサイズ(バイト単位)。それぞれのサイズは、特定のタイプを表しています。
0	dupb ブロックで使用されます。
4	DNS、ISAKMP、URL フィルタリング、uauth、TFTP、TCP モジュールなどのアプリケーションの既存ブロックを複製します。またこのサイズのブロックは、通常、パケットをドライバに送信するコードなどで使用されます。
80	TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。
256	ステートフル フェールオーバーの更新、syslog 処理、およびその他の TCP 機能に使用されます。 これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブな ASA は、パケットを生成してスタンバイ ASA に送信し、変換と接続のテーブルを更新します。接続が頻繁に作成または切断されるバーストトラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。この状況は、1 つまたはそれ以上の接続がスタンバイ ASA に対して更新されなかったことを示しています。ステートフル フェールオーバー プロトコルは、不明な変換または接続を次回に捕捉します。256 バイト ブロックの CNT カラムが長時間にわたって 0 またはその付近で停滞している場合は、ASA の処理している 1 秒あたりの接続数が非常に多いために、変換テーブルと接続テーブルの同期が取れている状態を ASA が維持できない問題が発生します。 ASA から送信される syslog メッセージも 256 バイト ブロックを使用しますが、256 バイト ブロック プールが枯渇するような量が発行されることは通常ありません。CNT カラムの示す 256 バイト ブロックの数が 0 に近い場合は、Debugging (レベル 7)のログを syslog サーバに記録していないことを確認してください。この情報は、ASA コンフィギュレーションの logging trap 行に示されています。ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification(レベル 5)以下に設定することを推奨します。
1550	ASA で処理するイーサネット パケットを格納するために使用されます。 パケットは、ASA インターフェイスに入ると入力インターフェイス キューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。ASA は、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいて決定し、パケットを発信インターフェイス上の出力キューに配置します。ASA がトラフィック負荷に対応できていない場合は、使用可能なブロックの数が 0 付近で停滞します(このコマンドの出力の CNT 列に示されます)。CNT 列が 0 の場合、ASA はより多くのブロックを割り当てようとします。このコマンドを実行すると、1550 バイト ブロックの最大数を 8192 より大きくすることができます。使用可能なブロックがなくなった場合、ASA はパケットをドロップします。
16384	64 ビット 66 MHz のギガビット イーサネット カード(i82543)にのみ使用されます。 イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御の更新に使用される制御フレームまたはガイド付きフレーム。

表 4-26　show blocks のフィールド(続き)

フィールド	説明
MAX	指定したバイト ブロックのプールで使用可能なブロックの最大数。起動時に、最大限のブロック数がメモリから切り分けられます。通常、ブロックの最大数は変化しません。例外は 256 バイト ブロックおよび 1550 バイト ブロックで、ASA は必要に応じてより多くのブロックをダイナミックに作成できます。このコマンドを実行すると、1550 バイト ブロックの最大数を 8192 より大きくすることができます。
LOW	低基準値。この数は、ASA の電源がオンになった時点、またはブロックが(**clear blocks** コマンドで)最後にクリアされた時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがいっぱいになったことを示します。
CNT	特定のサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在いっぱいであることを意味します。

次に、**show blocks all** コマンドの出力例を示します。

```
ciscoasa# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

表 4-27 に、各フィールドの説明を示します。

表 4-27　show blocks all のフィールド

フィールド	説明
ブロック	ブロックのアドレス。
allocd_by	ブロックを最後に使用したアプリケーションのプログラム アドレス(使用されていない場合は 0)。
freed_by	ブロックを最後に解放したアプリケーションのプログラム アドレス。
data size	ブロック内部のアプリケーション バッファまたはパケット データのサイズ。
alloccnt	このブロックが作成されてから使用された回数。
dup_cnt	このブロックに対する現時点での参照回数(このブロックが使用されている場合)。0 は 1 回の参照、1 は 2 回の参照を意味します。
oper	ブロックに対して最後に実行された操作。alloc、get、put、free の 4 つのいずれかです。
場所	ブロックを使用しているアプリケーション。または、ブロックを最後に割り当てたアプリケーションのプログラム アドレス(allocd_by フィールドと同じ)。

次に、コンテキスト内での **show blocks** コマンドの出力例を示します。

```
ciscoasa/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

次に、**show blocks queue history** コマンドの出力例を示します。

```
ciscoasa# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

次に、**show blocks queue history detail** コマンドの出力例を示します。

```
ciscoasa# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
```

```
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

次に、**show blocks pool summary** コマンドの出力例を示します。

```
ciscoasa# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

次に、**show blocks exhaustion history list** コマンドの出力例を示します。

```
ciscoasa# show blocks exhaustion history list
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
```

表 4-28 に、各フィールドの説明を示します。

表 4-28　show blocks pool summary のフィールド

フィールド	説明
total_count	指定したクラスのブロックの数。
miss_count	技術的な理由により、指定したカテゴリでレポートされなかったブロックの数。
Freed_pc	このクラスのブロックを解放したアプリケーションのプログラム アドレス。
Alloc_pc	このクラスにブロックを割り当てたアプリケーションのプログラム アドレス。
Queue	このクラスの有効なブロックが属しているキュー。
valid_cnt	現時点で割り当てられているブロックの数。
invalid_cnt	現時点では割り当てられていないブロックの数。
Invalid Bad qtype	このキューが解放されて内容が無効になっているか、このキューは初期化されていませんでした。
Valid tcp_usr_conn_inp	キューは有効です。

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられるメモリを増やします。
clear blocks	システム バッファの統計情報をクリアします。
show conn	アクティブな接続を表示します。

show bootvar

ブート ファイルとコンフィギュレーションのプロパティを表示するには、特権 EXEC モードで **show bootvar** コマンドを使用します。

show bootvar

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴d

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

BOOT 変数は、さまざまなデバイス上の起動イメージのリストを指定します。CONFIG_FILE 変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。これらの変数は、それぞれ **boot system** コマンドと **boot config** コマンドで設定します。

例

BOOT 変数は disk0:/f1_image を保持しています。これは、システムのリロード時にブートされるイメージです。BOOT の現在の値は、disk0:/f1_image; disk0:/f1_backupimage です。この値は、BOOT 変数が **boot system** コマンドで変更されているものの、実行コンフィギュレーションがまだ **write memory** コマンドで保存されていないことを意味しています。実行コンフィギュレーションを保存すると、BOOT 変数と現在の BOOT 変数が両方とも disk0:/f1_image; disk0:/f1_backupimage になります。実行コンフィギュレーションが保存済みである場合、ブートローダは BOOT 変数の内容をロードしようとします。つまり、disk0:/f1image を起動します。このイメージが存在しないか無効である場合は、disk0:1/f1_backupimage をブートしようとします。

CONFIG_FILE 変数は、システムのスタートアップ コンフィギュレーションを指します。この例ではこの変数が設定されていないため、スタートアップ コンフィギュレーション ファイルは、**boot config** コマンドで指定したデフォルトです。現在の CONFIG_FILE 変数は、**boot config** コマンドで変更して、**write memory** コマンドで保存できます。

次に、**show bootvar** コマンドの出力例を示します。

```
ciscoasa# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
ciscoasa#
```

関連コマンド

コマンド	説明
boot	起動時に使用されるコンフィギュレーション ファイルまたはイメージ ファイルを指定します。

show bridge-group

割り当てられたインターフェイス、MAC アドレス、IP アドレスなどブリッジ グループ情報を表示するには、特権 EXEC モードで **show bridge-group** コマンドを使用します。

show bridge-group *bridge_group_number*

構文の説明

bridge_group_number	ブリッジ グループ番号を 1 ～ 100 の整数で指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.7(1)	ルーテッド モードでの Integrated Routing and Bridging のサポートが追加されました。

例

次に、IPv4 アドレスを指定した **show bridge-group** コマンドの出力例を示します。

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

次に、IPv4 アドレスおよび IPv6 アドレスを指定した **show bridge-group** コマンドの出力例を示します。

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
    2000:101::1, subnet is 2000:101::/64
```

```
   2000:102::1, subnet is 2000:102::/64
Static mac-address entries: 0
Dynamic mac-address entries: 2
```

関連コマンド

コマンド	説明
bridge-group	トランスペアレント ファイアウォール インターフェイスをブリッジ グループにグループ化します。
clear configure interface bvi	ブリッジ グループ インターフェイス コンフィギュレーションをクリアします。
interface	インターフェイスを設定します。
interface bvi	ブリッジ仮想インターフェイスを作成します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
show running-config interface bvi	ブリッジ グループ インターフェイス コンフィギュレーションを表示します。

show call-home

設定した Call Home 情報を表示するには、特権 EXEC モードで **show call-home** コマンドを使用します。

[**cluster exec**] **show call-home** [**alert-group** | **detail** | **events** | **mail-server status** | **profile** {*profile _name* | **all**} | **statistics**]

構文の説明

alert-group	（任意）使用可能なアラート グループを表示します。
cluster exec	（オプション）クラスタリング環境では、あるユニットで **show call-home** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。
detail	（任意）Call Home コンフィギュレーションの詳細を表示します。
events	（任意）現在の検出されたイベントを表示します。
mail-server status	（任意）Call Home メール サーバのステータス情報を表示します。
profile *profile _name* **all**	（任意）すべての既存プロファイルのコンフィギュレーション情報を表示します。
statistics	（任意）Call Home の統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。
9.1(3)	**show cluster history** コマンドおよび **show cluster info** コマンドの出力を含めるために、Smart Call Home メッセージの新しいタイプが追加されました。

例

次に、設定された Call Home 設定を表示する **show call-home** コマンドの出力例を示します。

```
ciscoasa# show call-home
Current Smart Call-Home settings:
Smart Call-Home feature : enable
Smart Call-Home message's from address: from@example.com
Smart Call-Home message's reply-to address: reply-to@example.com
contact person's email address: example@example.com
contact person's phone: 111-222-3333
```

```
street address: 1234 Any Street, Any city, Any state, 12345
customer ID: ExampleCorp
contract ID: X123456789
site ID: SantaClara
Mail-server[1]: Address: smtp.example.com Priority: 1
Mail-server[2]: Address: 192.168.0.1 Priority: 10
Rate-limit: 60 message(s) per minute
Available alert groups:
Keyword                  State
------------------------ -------
Syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
Profiles:
Profile Name: CiscoTAC-1
Profile Name: prof1
Profile Name: prof2
```

次に、Call Home コンフィギュレーション情報の詳細を表示する **show call-home detail** コマンドの出力例を示します。

```
ciscoasa# show call-home detail
Description: Show smart call-home configuration in detail.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Current Smart Call-Home settings:
Smart Call-Home feature: enable
Smart Call-Home message's from address: from@example.example.com
Smart Call-Home message's reply-to address: reply-to@example.example.com
contact person's email address: abc@example.com
contact person's phone: 111-222-3333
street address: 1234 Any Street, Any city, Any state, 12345
customer ID: 111111
contract ID: 123123
site ID: SantaClara
Mail-server[1]: Address: example.example.com Priority: 1
Mail-server[2]: Address: example.example.com Priority: 10
Rate-limit: 60 message(s) per minute
Available alert groups:
Keyword State
------------------------ -------
syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
Profiles:
Profile Name: CiscoTAC-1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): anstage@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity
------------------------ ------------
inventory n/a
```

```
Profile Name: prof1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): example@example.com
HTTP address(es): https://kafan-lnx-01.cisco.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
Profile Name: prof2
Profile status: ACTIVE Preferred Message Format: short-text
Message Size Limit: 1048576 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
```

次に、使用可能な Call Home イベントを表示する **show call-home events** コマンドの出力例を示します。

```
ciscoasa# show call-home events
Description: Show current detected events.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Active event list:
Event client alert-group severity active (sec)
-------------------------------------------------------------------
Configuration Client configuration none 5
Inventory inventory none 15
```

次に、使用可能な Call Home メール サーバのステータスを表示する **show call-home mail-server status** コマンドの出力例を示します。

```
ciscoasa# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Mail-server[1]: Address: example.example.com Priority: 1 [Available]
Mail-server[2]: Address: example.example.com Priority: 10 [Not Available]
```

次に、使用可能なアラート グループを表示する **show call-home alert-group** コマンドの出力例を示します。

```
ciscoasa# show call-home alert-group
Description: Show smart call-home alert-group states.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Available alert groups:
Keyword State
------------------------ -------
syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
```

次に、**show call-home profile profile-name | all** コマンドの出力例と、すべての定義済みプロファイルおよびユーザ定義プロファイルに関する情報を示します。

```
ciscoasa# show call-home profile {profile-name | all}
Description: Show smart call-home profile configuration.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Profiles:
Profile Name: CiscoTAC-1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): anstage@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity
------------------------ ------------
inventory n/a
Profile Name: prof1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
Profile Name: prof2
Profile status: ACTIVE Preferred Message Format: short-text
Message Size Limit: 1048576 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
```

次に、Call Home の統計情報を表示する **show call-home statistics** コマンドの出力例を示します。

```
ciscoasa# show call-home statistics
Description: Show smart call-home statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Message Types Total Email HTTP
--------------------- ---------------- ---------------- ----------------
Total Success 0 0 0
Total In-Queue 0 0 0
Total Dropped 5 4 1
Tx Failed 5 4 1
inventory 3 2 1
configuration 2 2 0
Event Types Total
--------------------- ----------------
Total Detected 2
inventory 1
configuration 1
Total In-Queue 0
Total Dropped 0
Last call-home message sent time: 2009-06-17 14:22:09 GMT-07:00
```

次に、Call Home の統計情報を表示する **show call-home status** コマンドの出力例を示します。

```
ciscoasa# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Mail-server[1]: Address: kafan-lnx-01.cisco.com Priority: 1 [Available]
Mail-server[2]: Address: kafan-lnx-02.cisco.com Priority: 10 [Not Available]

37. ciscoasa# show call-home events
Description: Show current detected events.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Active event list:
Event client alert-group severity active (sec)
-----------------------------------------------------------------
Configuration Client configuration none 5
Inventory inventory none 15
```

次に、クラスタの Call Home の統計情報を表示する **cluster exec show call-home statistics** コマンドの出力例を示します。

```
ciscoasa(config)# cluster exec show call-home statistics
A(LOCAL):*******************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                 3                3                0
                test                 3                3                0

 Total In-Delivering                 0                0                0

      Total In-Queue                 0                0                0

Total Dropped                       8                8                0
           Tx Failed                8                8                0
        configuration               2                2                0
                test                6                6                0


Event Types             Total
--------------------   ----------------
      Total Detected               10
       configuration                1
                test                9

 Total In-Processing                0

      Total In-Queue                0

Total Dropped                       0

Last call-home message sent time: 2013-04-15 05:37:16 GMT+00:00

B:*******************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                 1                1                0
                test                 1                1                0

 Total In-Delivering                 0                0                0

      Total In-Queue                 0                0                0
```

```
Total Dropped                          2                2                0
          Tx Failed                    2                2                0
       configuration                   2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                   2
       configuration                   1
                test                   1

 Total In-Processing                   0

      Total In-Queue                   0

Total Dropped                          0

Last call-home message sent time: 2013-04-15 05:36:16 GMT+00:00

C:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                   0                0                0

 Total In-Delivering                   0                0                0

      Total In-Queue                   0                0                0

Total Dropped                          2                2                0
          Tx Failed                    2                2                0
       configuration                   2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                   1
       configuration                   1

 Total In-Processing                   0

      Total In-Queue                   0

Total Dropped                          0

Last call-home message sent time: n/a

D:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                   1                1                0
                test                   1                1                0

 Total In-Delivering                   0                0                0

      Total In-Queue                   0                0                0

Total Dropped                          2                2                0
          Tx Failed                    2                2                0
       configuration                   2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                   2
       configuration                   1
                test                   1
```

```
 Total In-Processing                  0

      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: 2013-04-15 05:35:34 GMT+00:00

ciscoasa(config)#
```

関連コマンド

コマンド	説明
call-home	Call Home コンフィギュレーション モードを開始します。
call-home send alert-group	特定のアラート グループ メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。

show call-home registered-module status

登録されたモジュールのステータスを表示するには、特権 EXEC モードで **show call-home registered-module status** コマンドを使用します。

show call-home registered-module status [**all**]

(注) [**all**] オプションは、システム コンテキスト モードでのみ有効です。

構文の説明

all	コンテキスト単位ではなく、デバイスに基づいてモジュール ステータスを表示します。マルチ コンテキスト モードでは、少なくとも 1 つのコンテキストでモジュールがイネーブルにされている場合、「**all**」オプションが含まれていれば、イネーブルにされていると表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

例

次に、**show call-home registered-module status all** の出力例を示します。

```
Output:
Module Name Status
-------------------------------------- --------------------
Smart Call-Home enabled
Failover Standby/Active
```

関連コマンド36.

コマンド	説明
call-home	Call Home コンフィギュレーション モードを開始します。
call-home send alert-group	特定のアラート グループ メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。

show capture

オプションを指定しない場合のキャプチャのコンフィギュレーションを表示するには、特権 EXEC モードで **show capture** コマンドを使用します。

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** ***number***] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

構文の説明

access-list *access_list_name*	(任意)特定のアクセス リスト ID の IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。
capture_name	(オプション)パケット キャプチャの名前を指定します。
cluster exec	(オプション)クラスタリング環境では、あるユニットで **show capture** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。
count *number*	(任意)指定されたデータのパケット数を表示します。
decode	このオプションは、isakmp タイプのキャプチャがインターフェイスに適用されている場合に役立ちます。当該のインターフェイスを通過する ISAKMP データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報とともに表示されます。
detail	(任意)各パケットについて、プロトコル情報を追加表示します。
dump	(オプション)データ リンク経由で転送されたパケットの 16 進ダンプを表示します。
packet-number *number*	指定したパケット番号から表示を開始します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(2)	IDS の出力に詳細情報が追加されました。
9.0(1)	**cluster exec** オプションが追加されました。
9.2(1)	出力で **vpn-user** ドメイン名が **filter-aaa** に変更されました。
9.3(1)	SGT およびイーサネット タギングの出力が追加されました。

リリース	変更内容
9.10(1)	GRE の IP 復号化および IPinIP カプセル化のサポートが追加されました。
9.13(1)	asp-drop のキャプチャタイプ向けの show capture が拡張され、drop のロケーションの詳細が含まれるようになりました。

使用上のガイドライン

capture_name を指定した場合は、そのキャプチャのキャプチャ バッファの内容が表示されます。

dump キーワードを指定しても、MAC 情報は 16 進ダンプに表示されません。

パケットのデコード出力は、パケットのプロトコルによって異なります。通常、このコマンドは、ICMP、UDP、および TCP プロトコルの IP デコードをサポートします。バージョン 9.10(1) から、このコマンドは、ICMP、UDP、および TCP についての GRE および IPinIP カプセル化の IP デコード出力の表示をサポートするように拡張されています。

表 4-29 で角カッコに囲まれている出力は、**detail** キーワードを指定した場合に表示されます。

表 4-29　パケット キャプチャの出力形式

パケット タイプ	キャプチャの出力形式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
『ARP』	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/GRE	**GRE でカプセル化された ICMP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source*> *carrier-ip-destination: gre:* [gre-flags] *ip-source* > *ip-destination: icmp: icmp-type icmp-code* [checksum-failure] **GRE でカプセル化された UDP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source*> *carrier-ip-destination: gre:* [gre-flags] *src-addr.src-port dest-addr.dst-port:* [checksum-info] *udp payload-len* **GRE でカプセル化された TCP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source*> *carrier-ip-destination: gre:* [gre-flags] *src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*

表 4-29　パケット キャプチャの出力形式(続き)

パケット タイプ	キャプチャの出力形式
IP/IPinIP	**IPinIP でカプセル化された ICMP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source*> *carrier-ip-destination: ipip-proto-4: ip-source* > *ip-destination: icmp: icmp-type icmp-code* [checksum-failure] **IPinIP でカプセル化された UDP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source*> *carrier-ip-destination: ipip-proto-4: src-addr.src-port dest-addr.dst-port:* [checksum-info] *udp payload-len* **IPinIP でカプセル化された TCP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source*> *carrier-ip-destination: ipip-proto-4: src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr*: *hex-dump*

ASA が不正な形式の TCP ヘッダー付きのパケットを受信し、*invalid-tcp-hdr-length* という ASP ドロップ理由のためにそのパケットをドロップした場合、そのパケットを受信したインターフェイスでは **show capture** コマンドの出力にパケットが表示されません。

バージョン 9.13(1) 以降、show capture の出力が拡張され、トラブルシューティングを容易にするために、asp-drop のキャプチャタイプが表示されたときにドロップ位置情報が含まれるようになりました。ASP ドロップ カウンタを使用したトラブルシューティングでは、同じ理由による ASP ドロップがさまざまな場所で使用されている場合は特に、ドロップの正確な位置は不明です。この情報は、ドロップの根本原因を特定する上で重要です。この拡張機能を使用すると、ビルド ターゲット、ASA リリース番号、ハードウェア モデル、および ASLR メモリ テキスト領域などの ASP ドロップの詳細が表示されます(ドロップの位置のデコードが容易になります)。

例

次に、キャプチャのコンフィギュレーションを表示する例を示します。

```
ciscoasa(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

次に、ARP キャプチャによってキャプチャされたパケットを表示する例を示します。

```
ciscoasa(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

次に、クラスタリング環境の 1 つのユニットでキャプチャされたパケットを表示する例を示します。

```
ciscoasa(config)# show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

次に、クラスタリング環境のすべてのユニットでキャプチャされたパケットを表示する例を示します。

```
ciscoasa(config)# cluster exec show capture
mycapture (LOCAL):--------------------------------------------------------

capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]

yourcapture:--------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

次に、次のコマンドを入力した後でクラスタリング環境のクラスタ制御リンクでキャプチャされたパケットの例を示します。

```
ciscoasa (config)# capture a interface cluster
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
ciscoasa (config)# capture cp interface cluster match udp any any eq 49495
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet 0/0

ciscoasa(config)# show capture
capture a type raw-data interface cluster [Capturing - 970 bytes]
capture cp type raw-data interface cluster [Capturing - 26236 bytes]
  match udp any eq 49495 any
capture dp type raw-data access-list cc1 interface cluster [Capturing - 4545230 bytes]
capture lacp type lacp interface gigabitEthernet0/0 [Capturing - 140 bytes]
```

次に、SGT とイーサネット タギングがインターフェイスでイネーブルになっている場合にキャプチャされたパケットの例を示します。

```
ciscoasa(config)# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

SGT とイーサネット タギングがインターフェイスでイネーブルの場合、インターフェイスは引き続きタグ付きパケットまたはタグなしパケットを受信できます。この例は、出力に INLINE-TAG 36 があるタグ付きパケット用です。同じインターフェイスがタグなしパケットを受信した場合も、出力は変わりません（つまり、「INLINE-TAG 36」エントリは出力に含まれません）。

次に、パケット トレーサによって生成される GRE、IPinIP、およびその他のパケット、およびインターフェイス内の後続のキャプチャ出力の例を示します。

GRE パケット：

```
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 icmp 1.1.1.1 8 0 2.2.2.2
```

IPinIP パケット：

```
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 icmp 1.1.1.1 8 0 2.2.2.2
```

通常の tcp/udp/icmp パケット：

```
packet-tracer input inside tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside icmp 1.1.1.1 8 0 2.2.2.2
```

```
ciscoasa(config)# show capture inside
12:10:37.523746       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1.1234 > 2.2.2.2.80: S
2145492151:2145492151(0) win 8192
12:10:37.623624       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1.1234 > 2.2.2.2.80:  udp 0
12:10:37.714471       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1 > 2.2.2.2 icmp: echo request
12:10:37.806690       31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1.1234 > 2.2.2.2.80: S
1501131661:1501131661(0) win 8192
12:10:37.897673       31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1.1234 > 2.2.2.2.80:  udp 0
12:10:41.974604       31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1 > 2.2.2.2 icmp: echo
request
12:16:14.957225       1.1.1.1.1234 > 2.2.2.2.80: S 2091733697:2091733697(0) win 8192
12:16:15.023909       1.1.1.1.1234 > 2.2.2.2.80:  udp 0
12:16:15.090449       1.1.1.1 > 2.2.2.2 icmp: echo request
```

（注） GRE および IPinIP パケットは、TCP/UDP/ICMP デコード機能を使用してデコードされ、内部パケットを表示します。

次の例は、このコマンドの出力に対する機能拡張を示しています。ドロップする場所のプログラムカウンタまたは現在の指示（後で復号化）、ビルドターゲット、ASA のリリース番号、ハードウェアモデル、および ASLR メモリのテキスト領域がキャプチャされて表示され、ドロップする場所の復号化を容易にします。

```
ciscoasa(config)# capture gtp_drop type asp-drop inspect-gtp

ciscoasa(config)# show capture gtp_drop [trace]
Target:         SSP
Hardware:   FPR4K-SM-12
Cisco Adaptive Security Appliance Software Version 9.13.1
ASLR enabled, text region 55cd421df000-55cd47530ea9
1 packets captured

1: 15:55:58.522983       192.168.108.12.41245 > 171.70.168.183.2123:  udp 27 Drop-reason:
(inspect-gtp) GTP inspection, Drop-location: frame 0x000055cd43db4019 flow (NA)/NA

ciscoasa(config)# show capture gtp_drop trace detail
Target:         SSP
Hardware:   FPR4K-SM-12
Cisco Adaptive Security Appliance Software Version 9.13.1
ASLR enabled, text region 55cd421df000-55cd47530ea9
1 packets captured

1: 15:55:58.522983 0050.56b0.bd99 5057.a884.2beb 0x0800 Length: 69
192.168.108.12.41245 > 171.70.168.183.2123:  [udp sum ok] udp 27 (ttl 64, id 53384)
Drop-reason: (inspect-gtp) GTP inspection, Drop-location: frame 0x000055cd43db4019 flow
(NA)/NA
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバにコピーします。

show chardrop

シリアル コンソールからドロップされた文字の数を表示するには、特権 EXEC モードで **show chardrop** コマンドを使用します。

show chardrop

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、**show chardrop** コマンドの出力例を示します。

```
ciscoasa# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。

show checkheaps

checkheaps に関する統計情報を表示するには、特権 EXEC モードで **show checkheaps** コマンドを使用します。チェックヒープは、ヒープ メモリ バッファの正常性およびコード領域の完全性を検証する定期的なプロセスです(ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられます)。

show checkheaps

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show checkheaps** コマンドの出力例を示します。

```
ciscoasa# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

関連コマンド

コマンド	説明
checkheaps	checkheap の確認間隔を設定します。

show checksum

コンフィギュレーションのチェックサムを表示するには、特権 EXEC モードで **show checksum** コマンドを使用します。

show checksum

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

show checksum コマンドを使用すると、コンフィギュレーションの内容のデジタル サマリーとして機能する 4 つのグループの 16 進数を表示できます。このチェックサムが計算されるのは、コンフィギュレーションをフラッシュ メモリに格納するときのみです。

show config コマンドまたは **show checksum** コマンドの出力でチェックサムの前にドット「.」が表示された場合、この出力は、通常のコンフィギュレーション読み込みまたは書き込みモードのインジケータを示しています（ASA のフラッシュ パーティションからの読み込み、またはフラッシュ パーティションへの書き込み時）。「.」は、ASA が操作ですでに占有されているが、「ハングアップ」しているわけではないことを示します。このメッセージは、「system processing, please wait」メッセージに似ています。

例

次に、コンフィギュレーションまたはチェックサムを表示する例を示します。

```
ciscoasa(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

チャンクに関する統計情報を表示するには、特権 EXEC モードで **show chunkstat** コマンドを使用します。

show chunkstat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、チャンクに関する統計情報を表示する例を示します。

```
ciscoasa# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
@ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
show cpu	CPU の使用状況に関する情報を表示します。

show class

クラスに割り当てられたコンテキストを表示するには、特権 EXEC モードで **show class** コマンドを使用します。

show class *name*

構文の説明

name	20 文字までの文字列で名前を指定します。デフォルト クラスを表示するには、名前として **default** と入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、**show class default** コマンドの出力例を示します。

```
ciscoasa# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス コンフィギュレーションをクリアします。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。

show clns

IS-IS の Connectionless Network Service（CLNS）情報を表示するには、特権 EXEC モードで **show clns** コマンドを使用します。

show clns {**filter-set** | **interface** [*interface_name*] | **is-neighbors** [*interface_name*] [**detail**] | **neighbors** [**areas**] [*interface_name*] [**detail**] | **protocol** [*domain*] | **traffic** [**since** {**bootup** | **show**}]}

構文の説明

エリア	（オプション）CLNS マルチエリア隣接関係を表示します。
ブートアップ	ブートアップ以降の CLNS プロトコル統計情報を表示します。
detail	（オプション）中継システムに関連付けられたエリアを表示します。そうでない場合は、サマリー表示が提供されます。
domain	（オプション）CLNS ドメインのルーティング プロトコル プロセス情報を表示します。
filter-set	CLNS フィルタ セットを表示します。
interface	CLNS インターフェイスのステータスと設定を表示します。
interface_name	（任意）インターフェイス名を指定します。
is-neighbors	IS ネイバー隣接関係を表示します。ネイバー エントリは、配置されているエリアに応じてソートされます。
ネイバー	エンド システム（ES）、中継システム（IS）、およびマルチトポロジ統合 Intermediate System-to-Intermediate System（M-ISIS）ネイバーを表示します。
protocol	CLNS ルーティング プロトコル プロセス情報を表示します。少なくとも 2 つのルーティング プロセス、レベル 1 およびレベル 2 が常に存在し、さらに多い場合もあります。
show	この **show** コマンドを最後に使用した以降の CLNS プロトコル統計情報を表示します。
since	（オプション）ブートアップ以降、またはこの **show** コマンドを最後に使用した以降のいずれかの CLNS プロトコル統計情報を表示します。
トラフィック	このルータが認識した CLNS パケットをリストします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは IS-IS の CLNS 情報を表示します。

例

以下の出力では、フィルタ セットが次のコマンドで定義されたものと仮定しています。

```
ciscoasa(config)# clns filter-set US-OR-NORDUNET 47.0005...
ciscoasa(config)# clns filter-set US-OR-NORDUNET 47.0023...
ciscoasa(config)# clns filter-set LOCAL 49.0003...
```

次に、**show clns filter-set** コマンドの出力例を示します。

```
ciscoasa# show clns filter-set

CLNS filter set US-OR-NORDUNET
      permit 47.0005...
      permit 47.0023...
CLNS filter set LOCAL
      permit 49.0003...
```

次に、トークン リングおよびシリアル インターフェイスの情報を含める **show clns interface** コマンドの出力例を示します。

```
ciscoasa# show clns interface
GigabitEthernet0/1 is up, line protocol is up
  Checksums enabled, MTU 1500
  ERPDUs enabled, min. interval 10 msec.
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 0 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 3
    Level-2 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 3
    Next IS-IS LAN Level-1 Hello in 1 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

表 4-30　show clns interface のフィールド

フィールド	説明
GigabitEthernet0/1 is up, line protocol is up	インターフェイスがアップで、ライン プロトコルがアップであることを示します。
Checksums enabled	イネーブルまたはディセーブルにできます。
MTU	最大伝送単位（MTU）の後ろにある数字は、このインターフェイスのパケットに対する最大伝送サイズです。

表 4-30　show clns interface のフィールド(続き)

フィールド	説明
ERPDUs	Error Protocol Data Unit（ERPDU）の生成に関する情報を表示します。イネーブルまたはディセーブルにできます。イネーブルの場合、指定された間隔よりも頻繁に送信されません。
RDPDUs	Redirect Protocol Data Unit（RDPDU）の生成に関する情報を表示します。イネーブルまたはディセーブルにできます。イネーブルの場合、指定された間隔よりも頻繁に送信されません。アドレス マスクがイネーブルの場合、リダイレクトがアドレス マスクで送信されます。
Congestion Experienced	CLNS がいつ輻輳検出ビットをオンにするのかを示します。デフォルトは、キュー内に 4 パケットを超えるパケットがある場合にこのビットがオンになります。
DEC compatibility mode	Digital Equipment Corporation（DEC）互換がイネーブルかどうかを示します。
Next ESH/ISH	次のエンド システム（ES）hello または中継システム（IS）hello がいつこのインターフェイスに送信されたかを示します。
Routing Protocol	このインターフェイスが属するエリアをリストします。通常、インターフェイスは 1 つのエリアのみに存在します。
Circuit Type	インターフェイスがローカル ルーティング（レベル 1）、エリア ルーティング（レベル 2）、またはローカルおよびエリア ルーティング（レベル 1-2）に対して設定されているかどうかを示します。
Interface number、local circuit ID、Level-1 Metric、DR ID、Level-1 IPv6 Metric、Number of active level-1 adjacencies、Level-2 Metric、DR ID、Level-2 IPv6 Metric、Number of active level-2 adjacencies、Next IS-IS LAN Level-1、Next IS-IS LAN Level-2	最後の一連のフィールドは、Intermediate System-to-Intermediate System（IS-IS）に関する情報を表示します。IS-IS に対して、レベル 1 およびレベル 2 メトリック、プロパティ、回線 ID、およびアクティブ レベル 1 およびレベル 2 隣接関係数が指定されます。
BFD enabled	BFD がインターフェイスでイネーブルです。

次に、**show clns is-neighbors** コマンドの出力例を示します。

```
ciscoasa# show clns is-neighbors

System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
```

表 4-31　show clns is-neighbors のフィールド

フィールド	説明
System Id	システムの ID 値。
インターフェイス	ルータが検出されるインターフェイス。
状態	隣接状態。Up および Init が状態です。show clns neighbors の説明を参照してください。
タイプ	L1、L2、および L1L2 タイプの隣接。**show clns neighbors** の説明を参照してください。
プライオリティ	関連ネイバーがアドバタイズしている IS-IS プライオリティ。インターフェイスの指定 IS-IS ルータに対して最もプライオリティの高いネイバーが選ばれます。
Circuit Id	指定 IS-IS ルータの何がインターフェイス用であるかのネイバーの認識。
書式	ネイバーがフェーズ V（OSI）隣接またはフェーズ IV（DECnet）隣接のいずれであるかを示します。

次に、**show clns is-neighbors detail** コマンドの出力例を示します。

```
ciscoasa# show clns is-neighbors detail

System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01         Phase V
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 00:12:49
  NSF capable
  Interface name: inside
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01         Phase V
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 00:12:50
  NSF capable
  Interface name: inside
```

次に、**show clns neighbors detail** コマンドの出力例を示します。

```
ciscoasa# show clns neighbors detail

System Id      Interface   SNPA                State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44      Up          26   L1L2
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
CSR7002        inside      000c.2906.491c      Up          27   L1L2
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
```

次に、**show clns neighbors** コマンドの出力例を示します。

```
ciscoasa# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44  Up         29    L1L2
CSR7002        inside      000c.2906.491c  Up         27    L1L2
```

表 4-32　show clns neighbors のフィールド

フィールド	説明
System Id	エリア内のシステムを識別する 6 バイト値。
インターフェイス	システムの学習元インターフェイス名。
SNPA	サブネットワーク接続点。これはデータ リンク アドレスです。
状態	ES、IS、または M-ISIS の状態。 • Init：システムは IS で、IS-IS hello メッセージを待機しています。IS-IS は、ネイバーを隣接関係にないと見なします。 • Up：ES または IS が到達可能であると確信しています。
Holdtime	この隣接関係エントリがタイムアウトするまでの秒数。
タイプ	隣接関係のタイプ。表示される可能性のある値は次のとおりです。 • ES：エンドシステム隣接関係が、ES-IS プロトコルを介して検出されたか、または静的に設定されました。 • IS：ルータ隣接関係が、ES-IS プロトコルを介して検出されたか、または静的に設定されました。 • M-ISIS：ルータ隣接関係が、マルチトポロジ IS-IS プロトコルを介して検出されました。 • L1：レベル 1 ルーティングのみのルータ隣接関係。 • L1L2：レベル 1 およびレベル 2 ルーティングのルータ隣接関係。 • L2：レベル 2 のみのルータ隣接関係。
Protocol	隣接関係が学習されたプロトコル。有効なプロトコル ソースは、ES-IS、IS-IS、ISO IGRP、Static、DECnet、および M-ISIS です。

次に、**show clns protocol** コマンドの出力例を示します。

```
ciscoasa# show clns protocol
IS-IS Router
  System Id: 0050.0500.5008.00  IS-Type: level-1-2
  Manual area address(es):
        49.0001
  Routing for area address(es):
        49.0001
  Interfaces supported by IS-IS:
        outside - IP
  Redistribute:
    static (on by default)
  Distance for L2 CLNS routes: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
```

次に、**show clns traffic** コマンドの出力例を示します。

```
ciscoasa# show clns traffic

CLNS:  Time since last clear: never
CLNS & ESIS Output: 0, Input: 8829
CLNS Local: 0, Forward: 0
CLNS Discards:
  Hdr Syntax: 0, Checksum: 0, Lifetime: 0, Output cngstn: 0
  No Route: 0, Discard Route: 0, Dst Unreachable 0, Encaps. Failed: 0
  NLP Unknown: 0, Not an IS: 0
CLNS Options: Packets 0, total 0 , bad 0, GQOS 0, cngstn exprncd 0
CLNS Segments:  Segmented: 0, Failed: 0
CLNS Broadcasts: sent: 0, rcvd: 0
Echos: Rcvd 0 requests, 0 replies
       Sent 0 requests, 0 replies
ESIS(sent/rcvd): ESHs: 0/0, ISHs: 0/0, RDs: 0/0, QCF: 0/0
Tunneling (sent/rcvd): IP: 0/0, IPv6: 0/0
Tunneling dropped (rcvd) IP/IPV6:  0
ISO-IGRP: Querys (sent/rcvd): 0/0 Updates (sent/rcvd): 0/0
ISO-IGRP: Router Hellos: (sent/rcvd): 0/0
ISO-IGRP Syntax Errors: 0

IS-IS: Time since last clear: never
IS-IS: Level-1 Hellos (sent/rcvd): 1928/1287
IS-IS: Level-2 Hellos (sent/rcvd): 1918/1283
IS-IS: PTP Hellos     (sent/rcvd): 0/0
IS-IS: Level-1 LSPs sourced (new/refresh): 7/13
IS-IS: Level-2 LSPs sourced (new/refresh): 7/14
IS-IS: Level-1 LSPs flooded (sent/rcvd): 97/2675
IS-IS: Level-2 LSPs flooded (sent/rcvd): 73/2628
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 CSNPs (sent/rcvd): 642/0
IS-IS: Level-2 CSNPs (sent/rcvd): 639/0
IS-IS: Level-1 PSNPs (sent/rcvd): 0/554
IS-IS: Level-2 PSNPs (sent/rcvd): 0/390
IS-IS: Level-1 DR Elections: 1
IS-IS: Level-2 DR Elections: 1
IS-IS: Level-1 SPF Calculations: 9
IS-IS: Level-2 SPF Calculations: 8
IS-IS: Level-1 Partial Route Calculations: 0
IS-IS: Level-2 Partial Route Calculations: 0
IS-IS: LSP checksum errors received: 0
IS-IS: Update process queue depth: 0/200
IS-IS: Update process packets dropped: 0
```

表 4-33　show clns traffic のフィールド

フィールド	説明
CLNS & ESIS Output	このルータが送信したパケットの合計数。
入力	このルータが受信したパケットの合計数。
CLNS Local	このルータによって生成されたパケット数をリストします。
Forward	このルータが転送したパケット数をリストします。
CLNS Discards	CLNS が廃棄したパケットとその廃棄理由をリストします。
CLNS Options	CLNS パケット内で見つかったオプションをリストします。
CLNS Segments	セグメント化されたパケットの数と、パケットをセグメント化できなかったことによって発生した障害数をリストします。

表 4-33　show clns traffic のフィールド(続き)

フィールド	説明
CLNS Broadcasts	送受信された CLNS ブロードキャストの数をリストします。
Echos	受信されたエコー要求パケットとエコー応答パケットの数をリストします。このフィールドの後ろの行には、送信されたエコー要求パケットとエコー応答パケットの数をリストします。
ESIS (sent/rcvd)	送受信されたエンド システム Hello(ESH)、中継システム Hello(ISH)、およびリダイレクトの数をリストします。
ISO IGRP	送受信された ISO Interior Gateway Routing Protocol(IGRP)のクエリーおよび更新の数を表示します。
Router Hellos	送受信された ISO IGRP ルータ hello パケットの数を表示します。
IS-IS: Level-1 hellos (sent/rcvd)	送受信されたレベル 1 IS-IS hello パケットの数を表示します。
IS-IS: Level-2 hellos (sent/rcvd)	送受信されたレベル 2 の IS-IS hello パケットの数を表示します。
IS-IS: PTP hellos (sent/rcvd)	シリアル リンクを通して送受信されたポイントツーポイントの IS-IS hello パケットの数を表示します。
IS-IS: Level-1 LSPs (sent/rcvd)	送受信されたレベル 1 のリンクステート プロトコル データ ユニット(PDU)の数を表示します。
IS-IS: Level-2 LSPs (sent/rcvd)	送受信されたレベル 2 のリンクステート PDU の数を表示します。
IS-IS: Level-1 CSNPs (sent/rcvd)	送受信されたレベル 1 Complete Sequence Number Packet(CSNP)の数を表示します。
IS-IS: Level-2 CSNPs (sent/rcvd)	送受信されたレベル 2 の CSNP の数を表示します。
IS-IS: Level-1 PSNPs (sent/rcvd)	送受信されたレベル 1 Partial Sequence Number Packet(PSNP)の数を表示します。
IS-IS: Level-2 PSNPs (sent/rcvd)	送受信されたレベル 2 の PSNP の数を表示します。
IS-IS: Level-1 DR Elections	レベル 1 の指定ルータの選定が行われた回数を表示します。
IS-IS: Level-2 DR Elections	レベル 2 の指定ルータの選定が行われた回数を表示します。
IS-IS: Level-1 SPF Calculations	レベル 1 の最短パス優先(SPF)ツリーが計算された回数を表示します。
IS-IS: Level-2 SPF Calculations	レベル 2 の SPF ツリーが計算された回数を表示します。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show clock

ASA に時刻を表示するには、ユーザ EXEC モードで **show clock** コマンドを使用します。

show clock [**detail**]

構文の説明

detail	(任意)クロック ソース(NTP またはユーザ コンフィギュレーション)と現在の夏時間設定(存在する場合)を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show clock** コマンドの出力例を示します。

```
ciscoasa# show clock
12:35:45.205 EDT Tue Jul 27 2004
```

次に、**show clock detail** コマンドの出力例を示します。

```
ciscoasa# show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

関連コマンド

コマンド	説明
clock set	ASA のクロックを手動で設定します。
clock summer-time	夏時間を表示する日付の範囲を設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show cluster

クラスタ全体の集約データまたはその他の情報を表示するには、特権 EXEC モードで **show cluster** コマンドを使用します。

show cluster [**chassis**] {**access-list** [*acl_name*] | **conn** [**count**] | **context** [*context_name*] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

構文の説明

access-list [*acl_name*]	アクセス ポリシーのヒット カウンタを示します。特定の ACL のカウンタを表示するには、*acl_name* と入力します。
chassis	Firepower 9300 ASA セキュリティ モジュールについて、シャーシのクラスタ情報を表示します。
conn [**count**]	使用中の接続の、すべてのユニットでの合計数を表示します。**count** キーワードを入力すると、接続数だけが表示されます。
context [*context_name*]	マルチコンテキストモードでのセキュリティコンテキストごとの使用状況を表示します。
cpu [**usage**]	CPU の使用率情報を表示します。
history	クラスタ スイッチング履歴を表示します。
interface-mode	クラスタ インターフェイス モードを表示します（spanned または individual）。
メモリ	システム メモリ使用率などの情報を表示します。
resource usage	システム リソースと使用状況を表示します。
service-policy	MPF サービス ポリシー統計情報を表示します。
トラフィック	トラフィック統計情報を表示します。
xlate count	現在の変換情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.4(1)	**service-policy** キーワードが追加されました。
9.4(1.152)	**chassis** キーワードが追加されました。
9.9(1)	**context** キーワードが追加されました。
9.14(1)	**履歴**出力が拡張され、トラブルシューティングの詳細が表示されるようになりました。

使用上のガイドライン

show cluster info コマンドおよび **show cluster user-identity** コマンドも参照してください。

例

次に、**show cluster access-list** コマンドの出力例を示します。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0, 0,
0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのユニットでの合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*****************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):*********************************************************
  100 in use, 100 most used

  cl1:*************************************************************
  100 in use, 100 most used
```

関連コマンド

コマンド	説明
show cluster info	クラスタ情報を表示します。
show cluster user-identity	クラスタ ユーザ ID 情報および統計情報を表示します。

show cluster info

クラスタ情報を表示するには、特権 EXEC モードで **show cluster info** コマンドを使用します。

show cluster info [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** [**details**] | **incompatible-config** | **loadbalance** | **load-monitor** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** {**asp** | **cp** [**detail**]} | **unit-join-acceleration incompatible-config**]

構文の説明

auto-join	(任意)一定時間遅延した後にクラスタ ユニットがクラスタに自動的に再参加するかどうか、および障害状態(ライセンスの待機やシャーシのヘルス チェック障害など)がクリアされたかどうかを示します。ユニットが永続的に無効になっている場合、またはユニットがすでにクラスタ内にある場合、このコマンドでは出力が表示されません。
clients	(オプション)登録クライアントのバージョンを表示します。
conn-distribution	(オプション)クラスタ内の接続分布を表示します。
flow-mobility counters	(オプション)EID の移動やフロー オーナーの移動に関する情報を表示します。
goid [*options*]	(オプション)グローバル オブジェクト ID データベースを示します。次のオプションがあります。 classmap conn-set hwidb idfw-domain idfw-group interface policymap virtual-context
health [**details**]	(オプション)ヘルス モニタリング情報を表示します。**details** キーワードは、ハートビート メッセージの失敗数を表示します。
incompatible-config	(オプション)現在の実行コンフィギュレーションのクラスタリングと互換性のないコマンドを表示します。このコマンドは、クラスタリングをイネーブルにする前に役立ちます。
loadbalance	(オプション)ロード バランシング情報を表示します。
load-monitor	(オプション)クラスタメンバのトラフィック負荷をモニタします。これには、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、**load-monitor** コマンドを使用してデフォルトで有効になっています。
old-members	(オプション)クラスタの以前のメンバーを表示します。
packet-distribution	(オプション)クラスタのパケット分布を表示します。

trace [*options*]	(オプション)クラスタリング制御モジュール イベント トレースを表示します。次のオプションがあります。 • **latest** [*number*]:最新の *number* のイベントを表示します。number は 1 ～ 2147483647 の範囲です。デフォルトではすべてが表示されます。 • **level** *level*:レベルでイベントをフィルタリングします。*level* は **all**、**critical**、**debug**、**informational**、**warning** のいずれかです。 • **module** *module*:モジュールでイベントをフィルタリングします。*module* は **ccp**、**datapath**、**fsm**、**general**、**hc**、**license**、**rpc**、**transport** のいずれかです。 • **time** {[*month day*] [*hh*:*mm*:*ss*]}:指定した時刻または日付より前のイベントを表示します。
transport {**asp** | **cp** [**detail**]}	(オプション)次のトランスポート関連の統計情報を表示します。 • **asp**:データ プレーンのトランスポート統計情報。 • **cp**:コントロール プレーン トランスポート統計情報。 **detail** キーワードを入力すると、クラスタで信頼性の高いトランスポート プロトコルの使用状況が表示され、バッファがコントロール プレーンでいっぱいになったときにパケット ドロップの問題を特定できます。
unit-join-acceleration incompatible-config	(オプション)**unit join-acceleration** コマンドが有効になっている場合(デフォルト)、一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。互換性のない設定を表示するには、**show cluster info unit-join-acceleration incompatible-config** コマンドを使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.3(1)	**show cluster info health** コマンドの改善されたモジュールのサポートが追加されました。
9.5(1)	サイト ID 情報が出力に追加されました。
9.5(2)	**flow-mobility counters** キーワードが追加されました。
9.8(1)	**health details** キーワードが追加されました。
9.9(2)	**auto-join** キーワードが追加されました。
9.9(2)	**transport cp** の **detail** キーワードが追加されました。
9.13(1)	**load-monitor** キーワードおよび **unit-join-acceleration incompatible-config** キーワードが追加されました。

使用上のガイドライン

オプションを指定しない場合、**show cluster info** コマンドはクラスタの名前とステータス、クラスタ メンバー、メンバーのステータスなど、一般的なクラスタ情報を表示します。

統計情報をクリアするには、**clear cluster info** コマンドを使用します。

show cluster コマンドおよび **show cluster user-identity** コマンドも参照してください。

例

次に、**show cluster info** コマンドの出力例を示します。

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Site ID : 1
      Version   : 9.5(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state SLAVE
      ID        : 1
      Site ID : 1
      Version   : 9.5(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Site ID : 2
      Version   : 9.5(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Site ID : 2
      Version   : 9.5(1)
```

```
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

次に、**show cluster info incompatible-config** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a user's
confirmation upon enabling clustering, can be removed automatically from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close

INFO: No manually-correctable incompatible configuration is found.
```

次に、**show cluster info trace** コマンドの出力例を示します。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

次に、ASA 5500-X での **show cluster info health** コマンドの出力例を示します。

```
ciscoasa# show cluster info health
Member ID to name mapping:
  0 - A   1 - B(myself)

                         0        1
GigabitEthernet0/0       up       up
Management0/0            up       up

ips (policy off)         up       None
sfr (policy off)         None     up
Unit overall             healthy   healthy
Cluster overall          healthy
```

上記の出力には、ASA IPS（ips）と ASA FirePOWER（sfr）の両方のモジュールが表示されます。モジュールごとに ASA は「policy on」または「policy off」を使用してサービス ポリシーが設定されたかどうかを示します。次に例を示します。

```
class-map sfr-class
    match sfr-traffic
policy-map sfr-policy
    class sfr-class
        sfr inline fail-close
service-policy sfr interface inside
```

上記の設定により、ASA FirePOWER モジュール（「sfr」）は「policy on」と表示されます。あるモジュールが、あるクラスタ メンバーでは「up」、他のメンバーでは「down」または「None」になっている場合、そのモジュールが down となっているメンバーはクラスタから除外されます。ただし、サービス ポリシーが設定されていない場合、クラスタ メンバーはクラスタから除外されません。モジュール ステータスは、モジュールが実行中である場合にのみ関連します。

次に、ASA 5585-X での **show cluster info health** コマンドの出力例を示します。

```
ciscoasa# show cluster info health
spyker-13# sh clu info heal
Member ID to name mapping:
  0 - A(myself) 1 - B

                       0 1
GigabitEthernet0/0       upup

SSM Card (policy off)    upup
Unit overall             healthyhealth
Cluster overall         healthyhealth
```

サービス ポリシーにモジュールを設定した場合は、出力に「policy on」と表示されます。サービス ポリシーを設定しない場合は、モジュールがシャーシに存在しても、出力に「policy off」と表示されます。

次に、**show cluster info flow-mobility counters** コマンドの出力例を示します。

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 0
EID movement notification processed : 0
Flow owner moving requested         : 0
```

次に、**show cluster info auto-join** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

show cluster info transport cp detail コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
```

```
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0
```

```
    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

```
MRT Tx of unitcast messages(to member_id:3)
=========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

次に、**show cluster info load-monitor** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

次に、**show cluster info unit-join-acceleration incompatible-config** コマンドの出力例を示します。

```
ciscoasa# show cluster info unit-join-acceleration incompatible-config
INFO: Clustering is not compatible with following commands. User must manually remove them
to activate the cluster unit join-acceleration feature.
zone sf200 passive
```

関連コマンド

コマンド	説明
show cluster	クラスタ全体の集約データを表示します。
show cluster user-identity	クラスタ ユーザ ID 情報および統計情報を表示します。

show cluster user-identity

クラスタ全体のユーザ ID 情報と統計情報を表示するには、特権 EXEC モードで **show cluster user-identity** コマンドを使用します。

show cluster user-identity {**statistics** [**user** *name* | **user-group** *group_name*] | **user** [**active** [**domain** *name*] | **user** *name* | **user-group** *group_name*] [**list** [*detail*] | **all** [**list** [*detail*] | **inactive** {**domain** *name* | **user-group** *group_name*] [**list** [*detail*]]}

構文の説明

active	アクティブな IP/ユーザ マッピングがあるユーザを表示します。
all	ユーザ データベース内のすべてのユーザを表示します。
domain *name*	ドメインのユーザ情報を表示します。
inactive	非アクティブな IP/ユーザ マッピングがあるユーザを表示します。
list [*detail*]	ユーザのリストを表示します。
statistics	クラスタ ユーザ ID 統計情報を表示します。
user	ユーザ データベースを表示します。
user *name*	特定のユーザの情報を表示します。
user-group *group_name*	特定のグループの各ユーザの情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show cluster info コマンドおよび **show cluster** コマンドも参照してください。

関連コマンド

コマンド	説明
show cluster	クラスタ全体の集約データを表示します。
show cluster info	クラスタ情報を表示します。

show cluster vpn-sessiondb distribution

クラスタ全体でアクティブおよびバックアップ セッションがどのように分散しているかを表示するには、特権 EXEC モードでこのコマンドを実行します。

show cluster vpn-sessiondb distribution

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.9(1)	このコマンドが追加されました。

使用上のガイドライン

この show コマンドを使用すると、各メンバーで **show vpn-sessiondb summary** を実行する必要なく、セッションのクイック ビューが提供されます。

各行には、メンバー ID、メンバー名、アクティブ セッション数、およびバックアップ セッションが存在するメンバーが含まれています。

例

たとえば、show cluster vpn-sessiondb distribution が以下のように出力された場合を考えます。

Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)

Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)

Member 2 (unit-1-2): active: 0

これは、次のように解釈できます。

- メンバー 0 には 209 のアクティブ セッションがあり、111 のセッションはメンバー 1 にバックアップされ、98 のセッションはメンバー 2 にバックアップされます。
- メンバー 1 には 204 のアクティブ セッションがあり、108 のセッションはメンバー 0 にバックアップされ、96 のセッションはメンバー 2 にバックアップされます。
- メンバー 2 にはアクティブ セッションがないため、クラスタ メンバーはこのノードのセッションをバックアップしていません。

関連コマンド

コマンド	説明
cluster redistribute vpn-sessiondb	分散型 VPN クラスタのアクティブな VPN セッションを再配布します。

show compression

ASA の圧縮統計情報を表示するには、特権 EXEC モードで **show compression** コマンドを使用します。

show compression [all | anyconnect-ssl | http-comp]

デフォルト

このコマンドにデフォルトの動作はありません。

構文の説明

all	すべての圧縮統計情報（anyconect-ssl、http comp）を表示
anyconnect-ssl	AnyConnect SSL 圧縮統計情報を表示します。
http-comp	HTTP-COMP 圧縮統計情報を表示

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

例

Show compression allでは次のタイプの統計情報が表示されます。

```
Compression AnyConnect Client Sessions              0
Compressed Frames                                   0
Compressed Data In (bytes)                          0
Compressed Data Out (bytes)                         0
Expanded Frames                                     0
Compression Errors                                  0
Compression Resets                                  0
Compression Output Buf Too Small                    0
Compression Ratio                                   0
Decompressed Frames                                 0
Decompressed Data In                                0
Decompressed Data Out                               0
Decompression CRC Errors                            0
Decompression Errors                                0
Decompression Resets                                0
Decompression Ratio                                 0
Block Allocation Failures                           0
Compression Skip Percent                           0%
Time Spent Compressing (peak)                    0.0%
```

```
Time Spent Decompressing (peak)                  0.0%
Number of http bytes in                            0
Number of http gzipped bytes out                   0
```

関連コマンド

コマンド	説明
圧縮	すべての SVC 接続および WebVPN 接続の圧縮をイネーブルにします。

show configuration

ASA でフラッシュ メモリに保存されているコンフィギュレーションを表示するには、特権 EXEC モードで **show configuration** コマンドを使用します。

show configuration

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。

使用上のガイドライン

show configuration コマンドは、ASA のフラッシュ メモリに保存されているコンフィギュレーションを表示します。**show running-config** コマンドとは異なり、**show configuration** コマンドの実行ではそれほど多くの CPU リソースが使用されません。

ASA のメモリ内のアクティブなコンフィギュレーション（保存されているコンフィギュレーションの変更など）を表示するには、**show running-config** コマンドを使用します。

例

次に、**show configuration** コマンドの出力例を示します。

```
ciscoasa# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
!
```

```
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.0.0.5 255.255.0.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
access-group mgcpacl in interface dmz
!
router ospf 1
 network 10.0.0.0 255.255.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
```

```
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
aaa authentication ssh console LOCAL
http server enable
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

関連コマンド

コマンド	説明
configure	ターミナルから ASA を設定します。

show configuration session

現在のコンフィギュレーション セッションおよびセッション内での変更を表示するには、特権 EXEC モードで **show configuration session** コマンドを使用します。

show configuration session [*session_name*]

構文の説明

session_name	既存のコンフィギュレーション セッションの名前。このパラメータを省略した場合、既存のすべてのセッションが表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ACL やその他のオブジェクトを編集するために隔離されたセッションを作成する、**configure session** コマンドとともに使用します。このコマンドは、セッション名と、そのセッションで行われたすべてのコンフィギュレーション変更を表示します。

コミット済みとして示されているセッションについて、変更が想定どおりに機能していないと判断した場合は、そのセッションを開いて、その変更を取り消すことができます。

例

次に、すべての使用可能なセッションの例を示します。

```
ciscoasa# show configuration session
config-session abc (un-committed)
 access-list abc permit ip any any
 access-list abc permit tcp any any
```

```
config-session abc2 (un-committed)
 object network test
 host 1.1.1.1
 object network test2
 host 2.2.2.2

ciscoasa#
```

関連コマンド

コマンド	説明
clear configuration session	コンフィギュレーション セッションとその内容を削除します。
clear session	コンフィギュレーション セッションの内容をクリアするか、そのアクセス フラグをリセットします。
configure session	セッションを作成するか、開きます。

show conn

指定した接続タイプの接続状態を表示するには、特権 EXEC モードで **show conn** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

show conn [**count** | [**all**] [**detail** [**data-rate-filter** {**lt** | **eq** | **gt**} *value*]] [**long**] [**state** *state_type*]
[**protocol** {**tcp** | **udp** | **sctp**}] [**scansafe**] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]]
[**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]]
[**port** *dest_port*[**-***dest_port*]]
[**user-identity** | **user** [*domain_nickname*\]*user_name* | **user-group**
[*domain_nickname*\\]*user_group_name*] | **security-group**] [**zone** *zone_name* [**zone** *zone_name*]
[...]] [**data-rate**]

構文の説明

address	(任意)指定した送信元 IP アドレスまたは宛先 IP アドレスとの接続を表示します。
all	(任意)通過トラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を表示します。
count	(任意)アクティブな接続の数を表示します。
dest_ip	(任意)宛先 IP アドレス(IPv4 または IPv6)を指定します。範囲を指定するには、IP アドレスをダッシュ(-)で区切ります。次に例を示します。 `10.1.1.1-10.1.1.5`
dest_port	(任意)宛先ポート番号を指定します。範囲を指定するには、ポート番号をダッシュ(-)で区切ります。次に例を示します。 `1000-2000`
detail	(任意)変換タイプとインターフェイスの情報を含め、接続の詳細を表示します。
data-rate-filter {**lt** | **eq** | **gt**} *value*	(オプション)データレート値(1 秒あたりのバイト数)に基づいてフィルタリングされた接続を表示します。次に例を示します。 `data-rate-filter gt 123`
long	(任意)接続をロング フォーマットで表示します。
netmask *mask*	(任意)指定された IP アドレスで使用するサブネット マスクを指定します。
port	(任意)指定した送信元ポートまたは宛先ポートとの接続を表示します。
protocol {**tcp** | **udp** | **sctp**}	(任意)接続プロトコルを指定します。
scansafe	(オプション)クラウド Web セキュリティ サーバに転送される接続を表示します。
security-group	(オプション)表示されるすべての接続が指定したセキュリティ グループに属することを指定します。
src_ip	(任意)送信元 IP アドレス(IPv4 または IPv6)を指定します。範囲を指定するには、IP アドレスをダッシュ(-)で区切ります。次に例を示します。 `10.1.1.1-10.1.1.5`
src_port	(任意)送信元ポートの番号を指定します。範囲を指定するには、ポート番号をダッシュ(-)で区切ります。次に例を示します。 `1000-2000`

state *state_type*	(任意)接続状態タイプを指定します。接続状態タイプに使用できるキーワードのリストについては、表 4-34 を参照してください。
user [*domain_nickname*\] *user_name*	(オプション)表示されるすべての接続が指定したユーザに属することを指定します。*domain_nickname* 引数が含まれていない場合、ASA はデフォルト ドメインのユーザに関する情報を表示します。
user-group [*domain_nickname*\\] *user_group_name*	(オプション)表示されるすべての接続が指定したユーザ グループに属することを指定します。*domain_nickname* 引数が含まれていない場合、ASA はデフォルト ドメインのユーザ グループに関する情報を表示します。
user-identity	(オプション)ASA がアイデンティティ ファイアウォール機能に対するすべての接続を表示することを指定します。接続を表示する場合、ASA は一致するユーザを識別するとそのユーザ名と IP アドレスを表示します。同様に、ASA は一致するホストを識別するとそのホスト名と IP アドレスを表示します。
zone [*zone_name*]	(オプション)ゾーンの接続を表示します。**long** キーワードと **detail** キーワードは、接続が構築されたプライマリ インターフェイスと、トラフィックの転送に使用される現在のインターフェイスを表示します。
data-rate	(オプション)データレート トラッキング ステータスが有効になっているか無効になっているかを表示します。

デフォルト

デフォルトでは、すべての通過接続が表示されます。デバイスへの管理接続も表示するには、**all** キーワードを使用する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	「ローカル」と「外部」ではなく、送信元と宛先の概念を使用するように、構文が簡易化されました。新しい構文では、送信元アドレスが入力された最初のアドレスで、宛先が 2 番目のアドレスです。以前の構文では、**foreign** や **fport** などのキーワードを使用して宛先アドレスおよびポートを設定していました。
7.2(5)/8.0(5)/8.1(2)/8.2(4)/8.3(2)	**tcp_embryonic** 状態タイプが追加されました。このタイプは、i フラグを伴うすべての TCP 接続(不完全接続)を表示します。UDP の i フラグ接続は表示されません。
8.2(1)	TCP ステート バイパスに b フラグが追加されました。
8.4(2)	アイデンティティ ファイアウォールをサポートするために、**user-identity**、**user**、および **user-group** キーワードが追加されました。

リリース	変更内容
9.0(1)	クラスタリングのサポートが追加されました。**scansafe** キーワードおよび **security-group** キーワードが追加されました。
9.3(2)	**zone** キーワードが追加されました。
9.5(2)	LISP フロー モビリティの対象となるトラフィックに L フラグが追加されました。
9.5(2)	Diameter 接続に、詳細な出力の Q フラグが追加されました。**protocol sctp** キーワードが追加されました。オフロードされたフローに、詳細な出力の o フラグが追加されました。
9.6(2)	STUN 接続に、詳細な出力の u フラグが追加されました。M3UA 接続に v フラグが追加されました。
9.7(1)	クラスタ ディレクタ ローカリゼーションの使用時にスタブ フローがローカル ディレクタ YI か、またはローカル バックアップ yI であることを示すため、I フラグが追加されました。
9.9(1)	detail 出力の最後に位置する VPN スタブは、そのクラスタのロールに加えて、接続が VPN 暗号化スタブ フローのロールを果たしていることを示します。
9.13(1)	DCD 対応接続用に、デッド接続検出（DCD）イニシエータ/レスポンダ プローブ カウントが **show conn detail** の出力に追加されました。
9.14(1)	接続データレート トラッキング ステータスが追加されました。 ユーザ指定のデータレート値によって接続をフィルタリングするために、**show conn detail** コマンドに **data-rate-filter** キーワードが追加されました。

使用上のガイドライン

show conn コマンドは、アクティブな TCP 接続および UDP 接続の数を表示し、さまざまなタイプの接続に関する情報を提供します。接続のテーブル全体を参照するには、**show conn all** コマンドを使用します。

（注） ASA で第 2 の接続を許すピンホールが作成された場合、このピンホールは、**show conn** コマンドでは不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

表 4-34 に、**show conn state** コマンドを使用するときに指定できる接続タイプを示します。複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。

表 4-34　接続状態のタイプ

キーワード	表示される接続タイプ
up	アップ状態の接続
conn_inbound	着信接続
ctiqbe	CTIQBE 接続
data_in	着信データ接続
data_out	発信データ接続
finin	FIN 着信接続

表 4-34　接続状態のタイプ(続き)

キーワード	表示される接続タイプ
finout	FIN 発信接続
h225	H.225 接続
h323	H.323 接続
http_get	HTTP get 接続
mgcp	MGCP 接続
nojava	Java アプレットへのアクセスを拒否する接続
rpc	RPC 接続
service_module	SSM によってスキャンされる接続
sip	SIP 接続
skinny	SCCP 接続
smtp_data	SMTP メール データ接続
sqlnet_fixup_data	SQL*Net データ インスペクション エンジン接続
tcp_embryonic	TCP 初期接続
vpn_orphan	孤立した VPN トンネル フロー

detail オプションを使用すると、表 4-35 に示した接続フラグを使用して、変換タイプとインターフェイスに関する情報が表示されます。また、**VPN スタブ**は、このコマンドの出力の最後に表示され、そのクラスタのロールに加えて、接続が VPN 暗号化スタブ フローのロールを果たしていることを示します。VPN スタブは非対称 VPN トラフィックのシナリオまたはハブ n スポークのシナリオで、クリア テキストのパケットを暗号化するために使用されます。

表 4-35　接続フラグ

Flag	説明
a	SYN に対する外部 ACK を待機
A	SYN に対する内部 ACK を待機
b	TCP ステート バイパス
B	外部からの初期 SYN
C	コンピュータ テレフォニー インターフェイス クイック バッファ エンコーディング(CTIQBE)メディア接続。
d	dump
D	DNS
E	外部バック接続。これは、内部ホストから開始されている必要があるセカンダリ データ接続です。たとえば、内部クライアントが PASV コマンドを発行し、外部サーバが受け入れた後、ASA は FTP を使用してこのフラグが設定された外部バック接続を事前割り当てします。内部クライアントがサーバに接続しようとすると、ASA はこの接続試行を拒否します。外部サーバだけが事前割り当て済みのセカンダリ接続を使用できます。
f	内部 FIN
F	外部 FIN
g	メディア ゲートウェイ コントロール プロトコル(MGCP)接続

表 4-35　接続フラグ（続き）

Flag	説明
G	接続がグループの一部。[1]
h	H.225
H	H.323
i	不完全な TCP 接続または UDP 接続
I	着信データ
k	Skinny Client Control Protocol（SCCP）メディア接続
K	GTP t3 応答
l	ローカル ディレクタ/バックアップ スタブ フロー
L	LISP フロー モビリティの対象となるトラフィック
m	SIP メディア接続
M	SMTP データ
o	オフロードされたフロー。
O	発信データ
p	複製（未使用）
P	内部バック接続。これは、内部ホストから開始されている必要があるセカンダリ データ接続です。たとえば、内部クライアントが PORT コマンドを発行し、外部サーバが受け入れた後、ASA は FTP を使用してこのフラグが設定された内部バック接続を事前割り当てします。外部サーバがクライアントに接続しようとすると、ASA はこの接続試行を拒否します。内部クライアントだけが事前割り当て済みのセカンダリ接続を使用できます。
q	SQL*Net データ
Q	Diameter 接続
r	確認応答された内部 FIN
R	TCP 接続に対する、確認応答された外部 FIN
R	UDP RPC[2]
s	外部 SYN を待機
S	内部 SYN を待機
t	SIP 一時接続[3]
T	SIP 接続[4]
u	STUN 接続
U	up
v	M3UA 接続
V	VPN の孤立
W	WAAS
X	CSC SSM などのサービス モジュールによって検査
y	クラスタリングの場合、バックアップ オーナー フローを識別します。
Y	クラスタリングの場合、ディレクタ フローを識別します。

表 4-35　接続フラグ(続き)

Flag	説明
z	クラスタリングの場合、フォワーダ フローを識別します。
Z	クラウド Web セキュリティ

1. G フラグは、接続がグループの一部であることを示します。制御接続および関連するすべてのセカンダリ接続を指定するために、GRE および FTP Strict 検査によって設定されます。制御接続が切断されると、関連するすべてのセカンダリ接続も切断されます。
2. **show conn** コマンド出力の各行は 1 つの接続(TCP または UDP)を表すため、1 行に 1 つの R フラグだけが存在します。
3. UDP 接続の場合、値 t は接続が 1 分後にタイムアウトすることを示しています。
4. UDP 接続の場合、値 T は、**timeout sip** コマンドを使用して指定した値に従って接続がタイムアウトすることを示しています。

(注)　DNS サーバを使用する接続の場合、**show conn** コマンドの出力で、接続の送信元ポートが *DNS サーバの IP アドレス*に置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル(送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル)が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は *app_id* で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答が ASA を通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドル タイマーが新しい DNS セッションによってリセットされているように見えます。これは共有 DNS 接続の性質によるものであり、仕様です。

(注)　**timeout conn** コマンドで定義した非アクティブ期間(デフォルトは 1:00:00)中に TCP トラフィックがまったく発生しなかった場合は、接続が終了し、対応する接続フラグ エントリも表示されなくなります。

LAN-to-LAN トンネルまたはネットワーク拡張モード トンネルがドロップし、回復しない場合は、孤立したトンネル フローが数多く発生します。このようなフローはトンネルのダウンによって切断されませんが、これらのフローを介して通過を試みるすべてのデータがドロップされます。**show conn** コマンドの出力では、このような孤立したフローを **V** フラグで示します。

次の TCP 接続方向性フラグが同じセキュリティ レベルのインターフェイス間の接続に適用された場合(**same-security permit** コマンドを参照)、同じセキュリティ レベルのインターフェイスでは「内部」または「外部」がないため、フラグの方向は無関係となります。ASA は、これらのフラグを同じセキュリティ レベルの接続で使用する必要があるため、ASA が、他の接続の特性に基づいて 1 つのフラグを別のフラグより優先して選択することがあります(たとえば、f 対 F)が、選択された方向性は無視する必要があります。

- B:外部からの初期 SYN
- a:SYN に対する外部 ACK を待機
- A:SYN に対する内部 ACK を待機
- f:内部 FIN
- F:外部 FIN
- s:外部 SYN を待機
- S:内部 SYN を待機

特定の接続に関する情報を表示するには、**security-group** キーワードを入力し、接続元と接続先の両方でセキュリティ グループ テーブル値またはセキュリティ グループ名を指定します。ASA は、指定のセキュリティ グループ テーブル値またはセキュリティ グループ名に一致する接続を表示します。

接続元および接続先のセキュリティ グループ テーブル値または接続元および接続先のセキュリティ グループ名を指定せずに **security-group** キーワードを指定すると、ASA はすべての SXP 接続のデータを表示します。

ASA は、接続データを *security_group_name* (*SGT_value*) の形式で表示するか、またはセキュリティ グループ名が不明な場合は単に *SGT_value* として表示します。

(注) スタブ接続が低速パスを通過しないため、セキュリティ グループ データはスタブ接続には使用できません。スタブ接続には、接続の所有者にパケットを転送するために必要な情報だけが保持されます。

単一のセキュリティ グループの名前を指定して、クラスタ内のすべての接続を表示できます。たとえば、次の例では、クラスタのすべてのユニットのセキュリティ グループ mktg に一致する接続が表示されます。

```
ciscoasa# show cluster conn security-group name mktg
```

接続データレートトラッキング機能の現在の状態(イネーブルまたはディセーブル)を表示するには、**data-rate** キーワードを使用します。**data-rate filter** キーワードを使用して、データレート値(1 秒あたりのバイト数)を基に接続をフィルタリングします。接続データをフィルタリングするには、比較演算子(より小さい、等しい、より大きい)を使用します。出力には、順方向と逆方向の両方のフローについて、アクティブな接続と 2 つのデータレート値(瞬時(1 秒)および最大データレート値)が表示されます。

例

複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。次に、アップ状態の RPC 接続、H.323 接続、および SIP 接続に関する情報を表示する例を示します。

```
ciscoasa# show conn state up,rpc,h323,sip
```

次に、**show conn count** コマンドの出力例を示します。

```
ciscoasa# show conn count
54 in use, 123 most used
```

次に、**show conn** コマンドの出力例を示します。次に、内部ホスト 10.1.1.15 から 10.10.49.10 の外部 Telnet サーバへの TCP セッション接続の例を示します。B フラグが存在しないため、接続は内部から開始されています。「U」、「I」および「O」フラグは、接続がアクティブであり、着信データと発信データを受信したことを示します。

```
ciscoasa# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
```

```
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

次に、**show conn** コマンドの出力例を示します。接続が SSM によってスキャンされていることを示す「X」フラグが含まれています。

```
ciscoasa# show conn address 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03, bytes 2733, flags UIOX
```

次に、**show conn detail** コマンドの出力例を示します。次に、外部ホスト 10.10.49.10 から内部ホスト 10.1.1.15 への UDP 接続の例を示します。D フラグは、DNS 接続であることを示しています。1028 は、接続上の DNS ID です。

```
ciscoasa# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       l - local director/backup stub flow
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up, u - STUN,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: asa1
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member

TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
```

```
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

次に、**show conn** コマンドの出力例を示します。**V** フラグで示されているとおり、孤立したフローが存在します。

```
ciscoasa# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

To limit the report to those connections that have orphan flows, add the **vpn_orphan** option to the **show conn state** command, as in the following example:

```
ciscoasa# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

クラスタリングの場合、接続フローをトラブルシューティングするには、最初にすべてのユニットの接続を一覧表示します。それには、マスター ユニットで **cluster exec show conn** コマンドを入力します。ディレクタ(Y)、バックアップ(y)、およびフォワーダ(z)のフラグを持つフローを探します。次の例には、3 つのすべての ASA での 172.18.124.187:22 から 192.168.103.131:44727 への SSH 接続が表示されています。ASA1 には z フラグがあり、この接続のフォワーダであることを表しています。ASA3 には Y フラグがあり、この接続のディレクタであることを表しています。ASA2 には特別なフラグはなく、これがオーナーであることを表しています。アウトバウンド方向では、この接続のパケットは ASA2 の内部インターフェイスに入り、外部インターフェイスから出ていきます。インバウンド方向では、この接続のパケットは ASA1 および ASA3 の外部インターフェイスに入り、クラスタ制御リンクを介して ASA2 に転送され、次に ASA2 の内部インターフェイスから出ていきます。

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO
```

```
ASA3:**************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0, flags
Y
```

ASA2 での **show conn detail** の出力は、最新のフォワーダが ASA1 であったことを示しています。

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 1 in use, 61 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       l - local director/backup stub flow
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up, u - STUN,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: asa1
  ID 1: asa2
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member

TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044, cluster sent/rcvd bytes
0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
        From most recent forwarder ASA1: 1032983 (41319 byte/s)
Traffic received at interface inside
        Locally received: 3061 (122 byte/s)
```

次に、アイデンティティ ファイアウォール機能の接続を表示する例を示します。

```
ciscoasa# show conn user-identity
1219 in use, 1904 most used
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00,
bytes 10, flags -
UDP inside (www.yahoo.com)10.0.0.2:1586 outside (user2)192.0.0.1:30000, idle 0:00:00,
bytes 10, flags –
UDP inside 10.0.0.34:1586 outside 192.0.0.25:30000, idle 0:00:00, bytes 10, flags –
…
```

```
ciscoasa# show conn user user1
2 in use
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00,
bytes 10, flags –
```

show conn long zone コマンドの次の出力を参照してください。

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080 inside-zone:inside1(inside2):
10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

detail キーワードを使用すると、デッド接続検出（DCD）プローブの情報が表示されます。この情報は、発信側と応答側で接続がプローブされた頻度を示します。たとえば、DCD 対応接続の接続詳細は次のようになります。

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828, cluster sent/rcvd bytes
0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

次の例では、接続データレートトラッキング機能のステータスを表示する方法について示します。

```
ciscoasa# show conn data-rate
Connection data rate tracking is currently enabled.
```

次の例では、指定したデータレートに基づいて接続をフィルタリングする方法について示します。

```
ciscoasa# show conn detail data-rate-filter ?

eq  Enter this keyword to show conns with data-rate equal to specified value
gt   Enter this keyword to show conns with data-rate greater than specified
       value
lt    Enter this keyword to show conns with data-rate less than specified value

ciscoasa# show conn detail data-rate-filter gt ?

<0-4294967295>  Specify the data rate value in bytes per second

ciscoasa# show conn detail data-rate-filter gt 123 | grep max rate
    max rate:     3223223/399628 bytes/sec
    max rate:     3500123/403260 bytes/sec
```

関連コマンド

コマンド	説明
clear conn	接続をクリアします。
clear conn data-rate	保存されている現在の最大データレートをクリアします。

show console-output

現在キャプチャされているコンソール出力を表示するには、特権 EXEC モードで **show console-output** コマンドを使用します。

show console-output

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show console-output** コマンドの出力例を示します。コンソール出力がない場合、次のメッセージが表示されます。

```
ciscoasa# show console-output
Sorry, there are no messages to display
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
clear configure timeout	コンフィギュレーションのアイドル時間継続時間をデフォルトに戻します。
console timeout	ASA に対するコンソール接続のアイドル タイムアウトを設定します。
show running-config console timeout	ASA に対するコンソール接続のアイドル タイムアウトを表示します。

show context

割り当てられているインターフェイス、コンフィギュレーション ファイルの URL、および設定済みコンテキストの数を含めてコンテキスト情報を表示するには（または、システム実行スペースからすべてのコンテキストのリストを表示するには）、特権 EXEC モードで **show context** コマンドを使用します。

show context [*name* | **detail** | **count**]

構文の説明

count	（任意）設定済みコンテキストの数を表示します。
detail	（任意）実行状態および内部使用のための情報を含めて、コンテキストに関する詳細な情報を表示します。
name	（任意）コンテキスト名を設定します。名前を指定しない場合、ASA はすべてのコンテキストを表示します。コンテキスト内で入力できるのは、現在のコンテキスト名のみです。

デフォルト

システム実行スペースでは、名前を指定しない場合、ASA はすべてのコンテキストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	割り当てられた IPS 仮想センサーについての情報が追加されました。

使用上のガイドライン

出力の説明については、「例」を参照してください。

例

次に、**show context** コマンドの出力例を示します。この例では、3 つのコンテキストが表示されています。

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
```

```
contexta          GigabitEthernet0/1.200        flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300        flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 4-36 に、各フィールドの説明を示します。

表 4-36　show context のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク(*)の付いているコンテキスト名は、管理コンテキストです。
インターフェイス	このコンテキストに割り当てられたインターフェイス。
URL	ASA がコンテキストのコンフィギュレーションをロードする URL。

次に、システム実行スペースでの **show context detail** コマンドの出力例を示します。

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

表 4-37 に、各フィールドの説明を示します。

表 4-37　コンテキストの状態

フィールド	説明
Context	コンテキストの名前。ヌル コンテキストの情報は内部でのみ使用されます。system というコンテキストは、システム実行スペースを表しています。
状態メッセージ:	コンテキストの状態。次に、表示される可能性のあるメッセージを示します。
Has been created, but initial ACL rules not complete	ASA はコンフィギュレーションを解析しましたが、デフォルト セキュリティ ポリシーを確立するためのデフォルト ACL をまだダウンロードしていません。デフォルト セキュリティ ポリシーは、すべてのコンテキストに対して最初に適用されるもので、下位セキュリティ レベルから上位セキュリティ レベルへのトラフィック送信を禁止したり、アプリケーション インスペクションおよびその他のパラメータをイネーブルにします。このセキュリティ ポリシーによって、コンフィギュレーションが解析されてからコンフィギュレーションの ACL がコンパイルされるまでの間に、トラフィックが ASA をいっさい通過しないことが保証されます。コンフィギュレーションの ACL は非常に高速でコンパイルされるため、この状態が表示されることはほとんどありません。
Has been created, but not initialized	**context** *name* コマンドを入力しましたが、まだ **config-url** コマンドを入力していません。
Has been created, but the config hasn't been parsed	デフォルトの ACL がダウンロードされましたが、まだ ASA がコンフィギュレーションを解析していません。この状態が表示される場合は、ネットワーク接続に問題があるために、コンフィギュレーションのダウンロードが失敗した可能性があります。または、**config-url** コマンドをまだ入力していません。コンフィギュレーションをリロードするには、コンテキスト内から **copy startup-config running-config** を入力します。システムから、**config-url** コマンドを再度入力します。または、ブランクの実行コンフィギュレーションの設定を開始します。
Is a system resource	この状態に該当するのは、システム実行スペースとヌル コンテキストのみです。ヌル コンテキストはシステムによって使用され、この情報は内部でのみ使用されます。
Is a zombie	**no context** コマンドまたは **clear context** コマンドを使用してコンテキストを削除しましたが、コンテキストの情報は、ASAがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Is active	このコンテキストは現在実行中であり、コンテキスト コンフィギュレーションのセキュリティ ポリシーに従ってトラフィックを通過させることができます。
Is ADMIN and active	このコンテキストは管理コンテキストであり、現在実行中です。
Was a former ADMIN, but is now a zombie	**clear configure context** コマンドを使用して管理コンテキストを削除しましたが、コンテキストの情報は、ASA がコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。

表 4-37　コンテキストの状態(続き)

フィールド	説明
Real Interfaces	このコンテキストに割り当てられたインターフェイス。インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、表示されるのはインターフェイスの実際の名前です。
Mapped Interfaces	インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、表示されるのはマッピングされた名前です。インターフェイスをマッピングしなかった場合は、実際の名前がもう一度表示されます。
Real IPS Sensors	AIP SSM をインストールしている場合に、コンテキストに割り当てられる IPS 仮想センサー。センサー名を **allocate-ips** コマンドでマッピングした場合、表示されるのはセンサーの実際の名前です。
Mapped IPS Sensors	センサー名を **allocate-ips** コマンドでマッピングした場合、表示されるのはマッピングされた名前です。センサー名をマッピングしなかった場合は、実際の名前がもう一度表示されます。
Flag	内部でのみ使用されます。
ID	このコンテキストの内部 ID。

次に、**show context count** コマンドの出力例を示します。

```
ciscoasa# show context count
Total active contexts: 2
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。

show controller

存在するすべてのインターフェイスについて、コントローラ固有の情報を表示するには、特権 EXEC モードで **show controller** コマンドを使用します。

show controller [**slot**] [*physical_interface*] [**pci** [**bridge** [*bridge-id* [*port-num*]]]] [**detail**]

構文の説明

bridge	（オプション）ASA 5585-X の PCI ブリッジ固有の情報を表示します。
bridge-id	（オプション）ASA 5585-X の一意の各 PCI ブリッジ ID を表示します。
detail	（任意）コントローラの詳細を表示します。
pci	（オプション）ASA 5585-X の PCI コンフィギュレーション領域の先頭 256 バイトとともに PCI デバイスの要約を表示します。
physical_interface	（任意）インターフェイス ID を指定します。
port-num	（オプション）ASA 5585-X 適応型 ASA の各 PCI ブリッジ内の一意のポート番号を表示します。
slot	（オプション）ASA 5580 の PCI-e バスおよびスロットの情報のみを表示します。

デフォルト

インターフェイスを指定しない場合、このコマンドはすべてのインターフェイスの情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	このコマンドは ASA 5505 のみではなく、すべてのプラットフォームに適用されるようになりました。**detail** キーワードが追加されました。
8.1(1)	ASA 5580 用に **slot** キーワードが追加されました。

リリース	変更内容
8.2(5)	IPS SSP がインストールされた ASA 5585-X 用に **pci**、**bridge**、*bridge-id*、*port-num* の各オプションが追加されました。また、すべての ASA モデル用に、ポーズ フレームを送信して 1 ギガビット イーサネット インターフェイスでのフロー制御を可能にするためのサポートが追加されました。
8.6(1)	ASA とソフトウェア モジュール間の制御トラフィックに使用される ASA 5512-X から ASA 5555-X Internal-Control0/0 までのインターフェイス用と、ASA とソフトウェア モジュールへのデータ トラフィックに使用される Internal-Data0/1 インターフェイス用に、**detail** キーワードのサポートが追加されました。

使用上のガイドライン

このコマンドは、内部的不具合やカスタマーにより発見された不具合を調査するときに、Cisco TAC がコントローラについての有用なデバッグ情報を収集するために役立ちます。実際の出力は、モデルとイーサネット コントローラによって異なります。このコマンドは、IPS SSP がインストールされている ASA 5585-X の対象となるすべての PCI ブリッジに関する情報も表示します。ASA サービス モジュール の場合、**show controller** コマンドの出力に PCIe スロット情報は表示されません。

例

次に、**show controller** コマンドの出力例を示します。

```
ciscoasa# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
         Port Ctrl-1:   0x0000  Vlan Map:      0x077f
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0080
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

     Global Registers:
         Control:       0x0482

-----------------------------------------------------------------------
Number of VLANs: 1
-----------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
-----------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
-----------------------------------------------------------------------

....
```

```
Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0002
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

...

Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                           0xe0004000 = 0x00000000
    ctrl_status                   0xe0004004 = 0x5501064a
    irq_src                       0xe0004008 = 0x00000000
    irq_msk                       0xe000400c = 0x00000000
    irq_hw_err_src                0xe0004010 = 0x00000000
    irq_hw_err_msk                0xe0004014 = 0x00001000
    bmu_cs_rxq                    0xe0004060 = 0x002aaa80
    bmu_cs_stxq                   0xe0004068 = 0x01155540
    bmu_cs_atxq                   0xe000406c = 0x012aaa80

   Bank 2: MAC address registers:

....
```

次に、**show controller detail** コマンドの出力例を示します。

```
ciscoasa# show controller gigabitethernet0/0 detail

GigabitEthernet0/0:
   Intel i82546GB revision 03

     Main Registers:
         Device Control:             0xf8260000 = 0x003c0249
         Device Status:              0xf8260008 = 0x00003347
```

```
    Extended Control:           0xf8260018 = 0x000000c0
    RX Config:                  0xf8260180 = 0x0c000000
    TX Config:                  0xf8260178 = 0x000001a0
    RX Control:                 0xf8260100 = 0x04408002
    TX Control:                 0xf8260400 = 0x000400fa
    TX Inter Packet Gap:        0xf8260410 = 0x00602008
    RX Filter Cntlr:            0xf8260150 = 0x00000000
    RX Chksum:                  0xf8265000 = 0x00000300

RX Descriptor Registers:
    RX Descriptor 0 Cntlr:      0xf8262828 = 0x00010000
    RX Descriptor 0 AddrLo:     0xf8262800 = 0x01985000
    RX Desccriptor 0 AddrHi:    0xf8262804 = 0x00000000
    RX Descriptor 0 Length:     0xf8262808 = 0x00001000
    RX Descriptor 0 Head:       0xf8262810 = 0x00000000
    RX Descriptor 0 Tail:       0xf8262818 = 0x000000ff
    RX Descriptor 1 Cntlr:      0xf8262828 = 0x00010000
    RX Descriptor 1 AddrLo:     0xf8260138 = 0x00000000
    RX Descriptor 1 AddrHi:     0xf826013c = 0x00000000
    RX Descriptor 1 Length:     0xf8260140 = 0x00000000
    RX Descriptor 1 Head:       0xf8260148 = 0x00000000
    RX Descriptor 1 Tail:       0xf8260150 = 0x00000000

TX Descriptor Registers:
    TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
    TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
    TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
    TX Descriptor 0 Length:     0xf8263808 = 0x00001000
    TX Descriptor 0 Head:       0xf8263810 = 0x00000000
    TX Descriptor 0 Tail:       0xf8263818 = 0x00000000

RX Address Array:
    Ethernet Address 0:         0012.d948.ef58
    Ethernet Address 1:         Not Valid!
    Ethernet Address 2:         Not Valid!
    Ethernet Address 3:         Not Valid!
    Ethernet Address 4:         Not Valid!
    Ethernet Address 5:         Not Valid!
    Ethernet Address 6:         Not Valid!
    Ethernet Address 7:         Not Valid!
    Ethernet Address 8:         Not Valid!
    Ethernet Address 9:         Not Valid!
    Ethernet Address a:         Not Valid!
    Ethernet Address b:         Not Valid!
    Ethernet Address c:         Not Valid!
    Ethernet Address d:         Not Valid!
    Ethernet Address e:         Not Valid!
    Ethernet Address f:         Not Valid!

PHY Registers:
    Phy Control:                0x1140
    Phy Status:                 0x7969
    Phy ID 1:                   0x0141
    Phy ID 2:                   0x0c25
    Phy Autoneg Advertise:      0x01e1
    Phy Link Partner Ability:   0x41e1
    Phy Autoneg Expansion:      0x0007
    Phy Next Page TX:           0x2801
    Phy Link Partnr Next Page:  0x0000
    Phy 1000T Control:          0x0200
    Phy 1000T Status:           0x4000
    Phy Extended Status:        0x3000
```

```
     Detailed Output - RX Descriptor Ring:

     rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
                 pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
     rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
                 pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000

    ........
```

次に、ASA 5512-X から ASA 5555-X までの内部インターフェイスに対する **show controller detail** コマンドの出力例を示します。

```
ciscoasa# show controller detail

Internal-Control0/0:
   ASA IPS/VM Back Plane TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap1
         Num of Transmit Rings : 1
         Num of Receive Rings  : 1
         Ring Size             : 128
         Max Frame Length      : 1550
         Out of Buffer         : 0
         Reset                 : 0
         Drop                  : 0
     Transmit Ring [0]:
         tx_pkts_in_queue      : 0
         tx_pkts               : 176
         tx_bytes              : 9664
     Receive Ring [0]:
         rx_pkts_in_queue      : 0
         rx_pkts               : 0
         rx_bytes              : 0
         rx_drops              : 0

Internal-Data0/1:
   ASA IPS/VM Management Channel TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap2
         Num of Transmit Rings : 1
         Num of Receive Rings  : 1
         Ring Size             : 128
         Max Frame Length      : 1550
         Out of Buffer         : 0
         Reset                 : 0
         Drop                  : 0
     Transmit Ring [0]:
         tx_pkts_in_queue      : 0
         tx_pkts               : 176
         tx_bytes              : 9664
     Receive Ring [0]:
         rx_pkts_in_queue      : 0
         rx_pkts               : 0
         rx_bytes              : 0
         rx_drops              : 0
```

次に、**show controller slot** コマンドの出力例を示します。

```
Slot  Card Description                                PCI-e Bandwidth Cap.
----  ----------------                                ---------------------
3.    ASA 5580 2 port 10GE SR Fiber Interface Card    Bus: x4, Card: x8

4.    ASA 5580 4 port GE Copper Interface Card        Bus: x4, Card: x4

5.    ASA 5580 2 port 10GE SR Fiber Interface Card    Bus: x8, Card: x8

6.    ASA 5580 4 port GE Fiber Interface Card         Bus: x4, Card: x4

7.    empty                                           Bus: x8

8.    empty                                           Bus: x8
```

次に、**show controller pci** コマンドの出力例を示します。

```
ciscoasa# show controller pci

PCI Evaluation Log:
  ------------------------------------------------------------------------------
    Empty

  PCI Bus:Device.Function (hex): 00:00.0 Vendor ID: 0x8086 Device ID: 0x3406
  ------------------------------------------------------------------------------

    PCI Configuration Space (hex):
    0x00: 86 80 06 34 00 00 10 00 22 00 00 06 10 00 00 00
    0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x20: 00 00 00 00 00 00 00 00 00 00 00 00 86 80 00 00
    0x30: 00 00 00 00 60 00 00 00 00 00 00 00 05 01 00 00
    0x40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x60: 05 90 02 01 00 00 00 00 00 00 00 00 00 00 00 00
    0x70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x90: 10 e0 42 00 20 80 00 00 00 00 00 00 41 3c 3b 00
    0xa0: 00 00 41 30 00 00 00 00 c0 07 00 01 00 00 00 00
    0xb0: 00 00 00 00 3e 00 00 00 09 00 00 00 00 00 00 00
    0xc0: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0xd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0xe0: 01 00 03 c8 08 00 00 00 00 00 00 00 00 00 00 00
    0xf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

    Link Capabilities: x4, Gen1
    Link Status: x4, Gen1
```

関連コマンド

コマンド	説明
show interface	インターフェイス統計情報を表示します。
show tech-support	Cisco TAC による問題の診断を可能にするような情報を表示します。

show coredump filesystem

コアダンプ ファイル システムの内容を表示するには、**show coredump filesystem** コマンドを入力します。

show coredump filesystem

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、コアダンプはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、コアダンプ ファイル システムの内容を表示します。

例

次に、**show coredump filesystem** コマンドを入力して、最近生成された任意のコアダンプの内容を表示する例を示します。

```
ciscoasa(config)# show coredump filesystem
Coredump Filesystem Size is 100 MB
Filesystem type is FAT for disk0
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/loop0 102182 75240 26942 74% /mnt/disk0/coredumpfsys
Directory of disk0:/coredumpfsys/
246 -rwx 20205386 19:14:53 Nov 26 2008 core_lina.2008Nov26_191244.203.11.gz
247 -rwx 36707919 19:17:27 Nov 26 2008 core_lina.2008Nov26_191456.203.6.gz
```

関連コマンド

コマンド	説明
coredump enable	コアダンプ機能をイネーブルにします。
clear configure coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプ ログをクリアします。コアダンプ ファイル システム自体での作業はないため、コアダンプ コンフィギュレーションが変更されたり、影響を受けたりすることはありません。
clear coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプ ログをクリアします。コアダンプ ファイルシステム自体での作業はないため、コアダンプ コンフィギュレーションが変更されたり、影響を受けたりすることはありません。
show coredump log	コアダンプ ログを表示します。

show coredump log

コアダンプ ログの内容を新しい順に表示するには、**show coredump log** コマンドを入力します。コアダンプ ログの内容を古い順に表示するには、**show coredump log reverse** コマンドを入力します。

show coredump log

show coredump log [**reverse**]

構文の説明

reverse	最も古いコアダンプ ログを表示します。

デフォルト

デフォルトでは、コアダンプはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、コアダンプ ログの内容を表示します。ログは、現在ディスク上にあるものを反映しています。

例

次に、これらのコマンドの出力例を示します。

```
ciscoasa(config)# show coredump log
[ 1 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
[ 2 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 5 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0'
```

(注) 新しいコアダンプ用の領域を確保するため、古いコアダンプ ファイルは削除されます。これは、コアダンプ ファイル システムがいっぱいになり、現在のコアダンプ用の領域が必要になった場合に、ASA によって自動的に行われます。このため、クラッシュが発生してコアダンプが上書きされないように、できるだけ早くコアダンプをアーカイブすることが不可欠となります。

```
ciscoasa(config)# show coredump log reverse
[ 1 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0''
[ 2 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 5 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
```

関連コマンド

コマンド	説明
coredump enable	コアダンプ機能をイネーブルにします。
clear configure coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプ ログをクリアします。コアダンプ ファイルシステム自体での作業はないため、コアダンプ コンフィギュレーションが変更されたり、影響を受けたりすることはありません。
clear coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプ ログをクリアします。コアダンプ ファイル システム自体での作業はないため、コアダンプ コンフィギュレーションが変更されたり、影響を受けたりすることはありません。
show coredump filesystem	コアダンプ ファイル システムの内容を表示します。

show counters

プロトコル スタック カウンタを表示するには、特権 EXEC モードで **show counters** コマンドを使用します。

show counters [all | context *context-name* **| summary | top** *N* **] [detail] [protocol** *protocol_name* **[:***counter_name***]] [threshold** *N***]**

構文の説明

all	フィルタの詳細を表示します。
context *context-name*	コンテキスト名を指定します。
:*counter_name*	カウンタを名前で指定します。
detail	詳細なカウンタ情報を表示します。
protocol *protocol_name*	指定したプロトコルのカウンタを表示します。
summary	カウンタの要約を表示します。
threshold *N*	指定したしきい値以上のカウンタのみを表示します。指定できる範囲は 1 ～ 4294967295 です。
top *N*	指定したしきい値以上のカウンタを表示します。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

show counters summary detail threshold 1

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.2(1)	イベント マネージャのカウンタが追加されました。
9.13(1)	Firepower 1000 および 2100 のアプライアンスモードに新しいカウンタ「HTTPERR」が追加されました。これは、FXOS への HTTP 要求メッセージタイムアウトの数を表します。

例

次に、すべてのカウンタを表示する例を示します。

```
ciscoasa# show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf

ciscoasa# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
IP           OUT_PKTS            411   Summary
IP           TO_ARP              105   Summary
IP           TO_UDP                9   Summary
UDP          IN_PKTS               9   Summary
UDP          DROP_NO_APP           9   Summary
FIXUP        IN_PKTS             202   Summary
UAUTH        IPV6_UNSUPPORTED     27   Summary
IDFW         HIT_USER_LIMIT        2   Summary
```

次に、カウンタの要約を表示する例を示します。

```
ciscoasa# show counters summary
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   Summary
IOS_IPC      OUT_PKTS              2   Summary
```

次に、コンテキストのカウンタを表示する例を示します。

```
ciscoasa# show counters context single_vf
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               4   single_vf
IOS_IPC      OUT_PKTS              4   single_vf
```

次に、イベント マネージャのカウンタを表示する例を示します。

```
ciscoasa# show counters protocol eem
Protocol     Counter           Value   Context
EEM          SYSLOG            22      Summary
EEM          COMMANDS          6       Summary
EEM          FILES             3       Summary
```

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタをクリアします。

show cpu

CPU の使用状況に関する情報を表示するには、特権 EXEC モードで **show cpu** コマンドを使用します。

[**cluster exec**] **show cpu** [**usage** *core-id* | **profile** | **dump** | **detailed**]

マルチ コンテキスト モードでは、システム コンフィギュレーションから次のように入力します。

[**cluster exec**] **show cpu** [**usage**] [**context** {**all** | *context_name*}]

構文の説明

all	すべてのコンテキストを表示することを指定します。
cluster exec	(オプション)クラスタリング環境では、あるユニットで **show cpu** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。
コンテキスト	1 つのコンテキストを表示することを指定します。
context_name	表示するコンテキストの名前を指定します。
core-id	プロセッサ コアの数を指定します。
detailed	(オプション)CPU の内部使用に関する詳細な情報を表示します。
dump	(オプション)TTY にダンプ プロファイリング データを表示します。
profile	(オプション)CPU プロファイリング データを表示します。
usage	(任意)CPU 使用状況を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために、*core-id* オプションが追加されました。
9.1(2)	**show cpu profile** コマンドと **show cpu profile dump** コマンドの出力が更新されました。
9.2(1)	仮想プラットフォームの CPU 使用状況が ASAv の出力に追加されました。

使用上のガイドライン

CPU 使用状況は、5 秒ごとの負荷の近似値を使用し、この概算値をさらに以降の 2 つの移動平均に適用することによって算出されます。

show cpu コマンドを使用すると、プロセス関連の負荷を検出できます（つまり、**show process** コマンドを、シングルモードとマルチ コンテキスト モードのシステム コンフィギュレーションの両方で実行した場合に表示される項目の代わりに、アクティビティを表示できます）。

さらに、マルチ コンテキスト モードでは、プロセス関連負荷を分散するよう、設定されたすべてのコンテキストで消費される CPU に要求できます。このためには、各コンテキストに変更して **show cpu** コマンドを入力するか、**show cpu context** コマンドを入力します。

プロセス関連の負荷は、最も近い整数に丸められますが、コンテキスト関連の負荷の場合は精度を表す 10 進数が 1 つ追加されます。たとえば、**show cpu** コマンドをシステム コンテキストから入力すると、**show cpu context system** コマンドを入力した場合とは異なる数値が示されます。前者は **show cpu context all** コマンドで表示される要約とほぼ同じですが、後者はその要約の一部にすぎません。

show cpu profile dump コマンドを **cpu profile activate** コマンドとともに使用して、CPU 問題のトラブルシューティング時に TAC が使用する情報を収集できます。**show cpu profile dump** コマンドの出力は、16 進形式です。

CPU プロファイラが開始条件の発生を待機している場合、**show cpu profile** コマンドは次の出力を表示します。

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

ASAv に関して、次のライセンス ガイドラインに注意してください。

- 許可される vCPU の数は、インストールされている vCPU プラットフォーム ライセンスによって決定されます。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数と一致する場合、状態は Compliant になります。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数を下回る場合、状態は Noncompliant: Over-provisioned になります。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数を超える場合、状態は Compliant: Under-provisioned になります。
- メモリ制限は、プロビジョニングされた vCPU の数によって決定されます。
  - プロビジョニングされたメモリが上限にある場合、状態は Compliant になります。
  - プロビジョニングされたメモリが上限を超える場合、状態は Noncompliant: Over-provisioned になります。
  - プロビジョニングされたメモリが上限を下回る場合、状態は Compliant: Under-provisioned になります。
- 周波数予約制限は、プロビジョニングされた vCPU の数によって決定されます。
  - 周波数予約メモリが必要最低限（1000 MHz）以上である場合、状態は Compliant になります。
  - 周波数予約メモリが必要最低限（1000 MHz）未満である場合、状態は Compliant: Under-provisioned になります。

たとえば、次の出力は、ライセンスが適用されていないことを示します。許可される vCPU の数はライセンスされた数を示し、Noncompliant: Over-provisioned は、製品がライセンスされたリソースよりも多いリソースを使用して実行されていることを示しています。

```
Virtual platform CPU resources
------------------------------
Number of vCPUs              :        1
Number of allowed vCPUs      :        0
vCPU Status                  :        Noncompliant: Over-provisioned
```

復号化する場合は、この情報をコピーし、TAC に提供します。

(注) ASA が FXOS シャーシで実行されている場合、**show cpu** コマンドの出力に表示される CPU コアの数が、Firepower 4100 プラットフォームや 9300（FXOS ベース）プラットフォームなど、一部のプラットフォームの **show version** コマンドの出力に表示される数よりも少ないことがあります。

動的なハイパースレッディングのサポートの導入により、Firepower 4100 プラットフォームおよび 9300 プラットフォームでの **show cpu** コマンドの出力が変更されました。トラフィックのスループットが低い場合、**show cpu [detailed | core | external]** CLI の出力は、スタンドアロンの ASA 出力に表示されるものと異なります。CPU ハイパースレッディング機能がディセーブルになっている場合、CPU コアの使用状況出力の後半部分は低くなります。ASA トラフィックのスループットがしきい値の上限を超えている場合、CPU ハイパースレッディング機能をイネーブルにすると **show cpu** コマンドがスタンドアロンの ASA と同じ出力を表示するようになります。

例

次に、CPU 使用状況を表示する例を示します。

```
ciscoasa# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

次に、CPU の使用状況に関する情報を表示する例を示します。

```
ciscoasa# show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)

Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%

CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%

Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

(注) 「Current control point elapsed versus the maximum control point elapsed for」という文は、コントロール ポイントの現在の負荷が、定義された期間内に検出された最大負荷と比較されることを意味します。これは絶対値ではなく比率です。5 秒間隔に対して 99% という数値は、コントロール ポイントの現在の負荷が、その 5 秒間隔における最大負荷の 99% であることを意味します。負荷が常に増加し続ける場合、負荷は常に 100% になります。ただし、最大絶対値が定義されていないため、実際の CPU には引き続き多くの空き容量がある可能性があります。

次に、マルチ モードでシステム コンテキストの CPU 使用状況を表示する例を示します。

```
ciscoasa# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

次に、すべてのコンテキストの CPU 使用状況を表示する例を示します。

```
ciscoasa# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

次に、「one」というコンテキストの CPU 使用状況を表示する例を示します。

```
ciscoasa/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

次の例では、プロファイラをアクティブ化して、1000 個のサンプルを格納するように指示します。

```
ciscoasa# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

次に、プロファイリングのステータス（in-progress および completed）の例を示します。

```
ciscoasa# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.

ciscoasa# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2

Process virtual address map:
---------------------------
…
---------------------------
End of process map
Samples for core 0 - stopped
{0x000000000007eadb6,0x000000000211ee7e} ...
```

次に、ASAv の CPU 使用状況の例を示します。

```
ciscoasa# show cpu
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

Virtual platform CPU resources
------------------------------
Number of vCPUs              :     2
Number of allowed vCPUs      :     2
vCPU Status                  :  Compliant

Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
```

```
Frequency Limit              :  4000 MHz
Maximum allowed              :  56000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :   136 MHz
```

次に、ASAv の CPU 使用状況の詳細の例を示します。

```
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 1       0.0 (0.0 + 0.0)  0.2 (0.2 + 0.0)  0.0 (0.0 + 0.0)
Core 2       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 3       0.0 (0.0 + 0.0)  0.1 (0.0 + 0.1)  0.0 (0.0 + 0.0)

Current control point elapsed versus the maximum control point elapsed for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%


CPU utilization of external processes for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%


Total CPU utilization for:
     5 seconds = 0.1%; 1 minute: 0.1%; 5 minutes: 0.1%

Virtual platform CPU resources
------------------------------
Number of vCPUs              :     4
Number of allowed vCPUs      :     4
vCPU Status                  :  Compliant

Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
Frequency Limit              :  20000 MHz
Maximum allowed              :  20000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :    99 MHz
```

ASA バージョン 9.6.1 以降、コントロールポイント（CP）の処理用に 2 つまたは 4 つのコアが選択され、使用可能なすべてのコアに CP が広がらないよう実行できるコア CP の数を制限します。トラフィック負荷がない場合でも、CP 処理用に選択されたコアは CPU ピンニングに一定の負荷がかかります。また、データパス（DP）スレッドをチェックするために各コアで DP をポーリングします。この負荷は **show cpu core** 出力には含まれていますが、**show cpu detail** 出力では除外されています。これは、show cpu detail によって CP および DP の負荷がチェックされるためです。

例

次の例に、**show cpu core** および **show cpu detail** コマンドの出力に含まれるさまざまな CPU 使用率値（Core 0 および Core 2）を示します。

```
ciscoasa(config)# show cpu core
Core 5 sec 1 min 5 min
Core 0 18.0% 18.0% 18.0%
Core 1 0.0% 0.0% 0.0%
Core 2 18.6% 18.5% 18.6%
Core 3 0.0% 0.0% 0.0%

ciscoasa(config)# show cpu detail

Break down of per-core data path versus control point cpu usage:
Core 5 sec 1 min 5 min
Core 0 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6)
```

```
Core 1 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0)
Core 2 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6)
Core 3 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0)
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
cpu profile activate	CPU プロファイリングをアクティベートします。

CHAPTER 5

show crashinfo コマンド～ show curpriv コマンド

show crashinfo

フラッシュ メモリに格納されている最新のクラッシュ情報ファイルの内容を表示するには、特権 EXEC モードで **show crashinfo** コマンドを使用します。

show crashinfo [**save**]

構文の説明

save	（任意）クラッシュ情報をフラッシュ メモリに保存するように ASA が設定されているかどうかを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(5)	出力に **show process** コマンド内のスレッド ID（TID）が表示されるようになりました。

リリース	変更内容
9.4(1)	出力には、生成された syslog の最新の 50 行が表示されます。これらの結果を表示できるようにするには、**logging buffer** コマンドをイネーブルにする必要があります。
9.7(1)	最新のシステム生成クラッシュ ファイルのみを表示するように出力が更新されました。

使用上のガイドライン

クラッシュ ファイルがテスト クラッシュから生成された（**crashinfo test** コマンドで生成された）場合、クラッシュ ファイルの最初のストリングは「**: Saved_Test_Crash**」であり、最後のストリングは「**: End_Test_Crash**」です。クラッシュ ファイルが実際のクラッシュから生成されたる場合、クラッシュ ファイルの最初の行の文字列は「**: Saved_Crash**」で、最後の文字列は「**: End_Crash**」です（**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドを使用して発生させたクラッシュを含む）。

クラッシュ データがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュ データをクリアしていた場合は、**show crashinfo** コマンドを実行するとエラー メッセージが表示されます。

（注） **crashinfo test** コマンドを使用した結果としてフラッシュ メモリに書き込まれたクラッシュ情報は、このコマンドの出力に表示できません。実際のクラッシュ ファイルのみが *crashinfo_YYYYMMDD_HHMMSS 5_UTC* の形式で表示されます。

例

次に、現在のクラッシュ情報コンフィギュレーションを表示する例を示します。

```
ciscoasa# show crashinfo save
crashinfo save enable
```

次に、クラッシュ ファイル テストの出力例を示します（このテストによって、ASA が実際にクラッシュすることはありません。このテストで提供されるのは、シミュレートされたサンプル ファイルです）。

```
ciscoasa(config)# crashinfo test
ciscoasa(config)# exit
ciscoasa# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)

Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
```

```
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
F-flags  : 0x2
F-flags2 : 0x0
F-flags3 : 0x10000
F-flags4 : 0x0
F-bytes  : 0
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
```

```
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
```

```
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
```

```
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used
```

```
------------------ show vpn-sessiondb summary ------------------

Active Session Summary

Sessions:
                           Active : Cumulative : Peak Concurrent : Inactive
  SSL VPN               :       2 :          2 :               2
    Clientless only     :       0 :          0 :               0
    With client         :       2 :          2 :               2 :        0
  Email Proxy           :       0 :          0 :               0
  IPsec LAN-to-LAN      :       1 :          1 :               1
  IPsec Remote Access   :       0 :          0 :               0
  VPN Load Balancing    :       0 :          0 :               0
  Totals                :       3 :          3

License Information:
  Shared VPN License Information:
    SSL VPN                     :     1500
      Allocated to this device :       50
      Allocated in network     :       50
      Device limit             :      750

  IPsec   :    750    Configured :    750    Active :      1    Load :   0%
  SSL VPN :     52    Configured :     52    Active :      2    Load :   4%
                          Active : Cumulative : Peak Concurrent
  IPsec               :         1 :          1 :               1
  SSL VPN             :         2 :         10 :               2
    AnyConnect Mobile :         0 :          0 :               0
    Linksys Phone     :         0 :          0 :               0
  Totals              :         3 :         11

Tunnels:
                     Active : Cumulative : Peak Concurrent
  IKE         :          1 :          1 :               1
  IPsec       :          1 :          1 :               1
  Clientless  :          2 :          2 :               2
  SSL-Tunnel  :          2 :          2 :               2
  DTLS-Tunnel :          2 :          2 :               2
  Totals      :          8 :          8
------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
```

```
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------

PC  SP       STATE    Runtime  SBASE Stack              Process   TID
Hsi 001e3329 00763e7c 0053e5c8 0     00762ef4 3784/4096 arp_timer 0x000000000000000a
Lsi 001e80e9 00807074 0053e5c8 0     008060fc 3792/4096 FragDBGC  0x000000000000006b
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPsec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
```

```
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

関連コマンド

コマンド	説明
clear crashinfo	すべてのクラッシュ情報ファイル、クラッシュ ファイルの内容を削除します。
crashinfo force	ASA を強制的にクラッシュさせます。
crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
crashinfo test	ASA でフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo files	最後の 5 つのクラッシュ情報ファイルを日付とタイムスタンプに基づいて表示します。

show crashinfo console

crashinfo console コマンドのコンフィギュレーション設定を表示するには、**show crashinfo console** コマンドを入力します。

show crashinfo console

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。

使用上のガイドライン

FIPS 140-2 に準拠していることにより、キーやパスワードなどのクリティカル セキュリティ パラメータをクリプト境界（シャーシ）の外側に配布することが禁止されています。アサートまたはチェックヒープのエラーによってデバイスがクラッシュしたとき、コンソールにダンプされるスタック領域やメモリ領域には、機密データが含まれていることがあります。この出力は、FIPS モードでは表示されないようにする必要があります。

例

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。

コマンド	説明
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシー チェックをイネーブルまたはディセーブルにします。
show running-config fips	ASA で実行されている FIPS コンフィギュレーションを表示します。

show crashinfo files

最新のシステム生成のクラッシュ ファイルを ASA に表示するには、特権 EXEC モードで **show crashinfo files** コマンドを使用します。出力には、フラッシュ メモリに書き込まれた最大 5 つのクラッシュ ファイルが日付とタイムスタンプに基づいて表示されます。クラッシュ ファイルがない場合、コマンド出力に情報は表示されません。

show crashinfo files

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

crashinfo test コマンドを使用した結果として、フラッシュ メモリに書き込まれたクラッシュ情報は、**show crashinfo files** の出力に表示できません。実際のクラッシュ ファイルのみが *crashinfo_YYYYMMDD_HHMMSS 5_UTC* の形式で表示されます。クラッシュ データがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュ データをクリアしていた場合は、**show crashinfo files** コマンドを実行するとエラー メッセージが表示されます。

例

次に、実際のクラッシュ情報ファイルを表示する例を示します。

```
ciscoasa# show crashinfo files

crashinfo_20160725_012315_UTC
crashinfo_20160725_021353_UTC
crashinfo_20160725_022309_UTC
crashinfo_20160725_024205_UTC
```

関連コマンド

コマンド	説明
clear crashinfo	すべてのクラッシュ ファイルの内容を削除します。
crashinfo force	ASA を強制的にクラッシュさせます。
crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
show crashinfo	最新のクラッシュ ファイルの内容を表示します。
crashinfo test	ASA でフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。

show crypto accelerator load-balance

ハードウェア暗号化アクセラレータ MIB 内のグローバルなロードバランシング情報またはアクセラレータ固有のロードバランシング情報を表示するには、**show crypto accelerator load-balance** コマンドを使用します。

show crypto accelerator load-balance [ipsec | ssl | detail [ipsec | ssl]]

構文の説明

detail	（任意）詳細情報を表示します。このオプションの後に、ipsec または ssl キーワードを含めることができます。
ipsec	（任意）暗号化アクセラレータ IPSec ロードバランシングの詳細を表示します。
ssl	（任意）暗号化アクセラレータ SSL ロードバランシングの詳細を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

```
T@@@@@@@@@@@@@@@@@@@@..............................  36.50% : _bn_mul_add_words
@@@@@@@@@@.....................................  19.75% : _bn_sqr_comba8
```

show crypto accelerator statistics

ハードウェア クリプト アクセラレータ MIB 内のグローバルな統計情報またはアクセラレータ固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto accelerator statistics** コマンドを使用します。

show crypto accelerator statistics

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

出力統計情報は、次のように定義されます。

Accelerator 0 はソフトウェア ベースの暗号エンジンの統計情報を示します。

Accelerator 1 はハードウェア ベースの暗号エンジンの統計情報を示します。

RSA 統計情報には、デフォルトでソフトウェアで実行される、2048 ビット キーの RSA 処理が表示されます。つまり、2048 ビット キーがある場合、IKE/SSL VPN は、IPsec/SSL ネゴシエーション フェーズ中にソフトウェアで RSA 処理を実行します。実際の IPsec/SSL トラフィックは、引き続きハードウェアを使用して処理されます。これにより、同時に開始された同時セッションが数多くある場合、CPU の高使用となります。このため、RSA キー処理が複数発生し、CPU の高使用となる可能性があります。このようにして CPU の高使用状態となった場合は、1024 ビット キーを使用して、ハードウェアで RSA キー処理を実行する必要があります。このためには、アイデンティティ証明書を再度登録する必要があります。リリース 8.3(2) 以降では、5510 から 5550 のプラットフォームで crypto engine large-mod-accel コマンドを使用して、ハードウェアでこれらの処理を実行することもできます。

2048 ビットの RSA キーを使用しており、ソフトウェアで RSA 処理が実行されている場合は、CPU プロファイリングを使用して、CPU の高使用状況の原因となっている関数を特定できます。通常、bn_* 関数と BN_* 関数は RSA に使用される大規模なデータ セットでの数学的処理であり、ソフトウェアでの RSA 処理中に CPU の使用状況を確認する場合に最も役立ちます。次に例を示します。

```
@@@@@@@@@@@@@@@@@@@@..............................  36.50% : _bn_mul_add_words
@@@@@@@@@@.....................................  19.75% : _bn_sqr_comba8
```

Diffie-Hellman 統計情報には、ソフトウェアで 1024 より大きいモジュラス サイズの暗号処理が実行されたことが表示されます（DH5（Diffie-Hellman グループ 5 が 1536 を使用しています）など）。この場合、2048 ビット キー証明書はソフトウェアで処理されます。このため、数多くのセッションが実行されるときに CPU の高使用状況となります。

（注） ASA 5505（Cavium CN505 プロセッサ搭載）のみが、ハードウェアにより高速化される 768 ビットおよび 1024 ビットのキー生成の Diffie-Hellman グループ 1 および 2 をサポートしています。Diffie-Hellman グループ 5（1536 ビットのキー生成）は、ソフトウェアで実行されます。

適応型セキュリティ アプライアンスでは 1 つの暗号エンジンが IPsec 処理および SSL 処理を実行します。起動時にハードウェア クリプト アクセラレータにロードされたクリプト（Cavium）マイクロコードのバージョンを表示するには、**show version** コマンドを入力します。次に例を示します。

```
ciscoasa(config) show version

Cisco Adaptive Security Appliance Software Version 8.0(4)8
Device Manager Version 6.1(5)
Compiled on Wed 15-Oct-09 17:27 by builders
System image file is "disk0:/interim/asa804-8-k8.bin"
Config file at boot was "startup-config"
asa up 5 days 17 hours
Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 512MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.05
```

DSA 統計情報には、2 つのフェーズでのキー生成が表示されます。最初のフェーズは、アルゴリズム パラメータの選択です。このパラメータは、システムの他のユーザと共有することがあります。2 番めのフェーズは、1 人のユーザ用の秘密キーと公開キーの算出です。

SSL 統計情報には、ハードウェア クリプト アクセラレータへの SSL トランザクションで使用される、プロセッサ集約的な公開キーの暗号化アルゴリズムに関するレコードが表示されます。

RNG 統計情報には、キーとして使用する同じ乱数のセットを自動的に生成できる送信元とレシーバに関するレコードが表示されます。

例

次に、グローバル コンフィギュレーション モードでグローバルなクリプト アクセラレータ統計情報を表示する例を示します。

```
ciscoasa # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
```

```
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
```

```
Total dropped packets: 0
[Input statistics]
   Input packets: 700
   Input bytes: 753544
   Input hashed packets: 700
   Input hashed bytes: 736400
   Decrypted packets: 700
   Decrypted bytes: 719944
[Output statistics]
   Output packets: 700
   Output bad packets: 0
   Output bytes: 767552
   Output hashed packets: 700
   Output hashed bytes: 744800
   Encrypted packets: 700
   Encrypted bytes: 728352
[Diffie-Hellman statistics]
   Keys generated: 97
   Secret keys derived: 1
[RSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
   Encrypted packets: 0
   Encrypted bytes: 0
   Decrypted packets: 0
   Decrypted bytes: 0
[DSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
[SSL statistics]
   Outbound records: 0
   Inbound records: 0
[RNG statistics]
   Random number requests: 1
   Random number request failures: 0
```

次の表に、各出力エントリの説明を示します。

出力	説明
Capacity	このセクションは、ASA がサポートできるクリプト アクセラレーションに関連しています。
Supports hardware crypto	(True/False) ASA はハードウェア クリプト アクセラレーションをサポートできます。
Supports modular hardware crypto	(True/False) サポートされている任意のハードウェア クリプト アクセラレータを個別のプラグイン カードまたはモジュールとして挿入できます。
Max accelerators	ASA でサポートされるハードウェア クリプト アクセラレータの最大数。
Mac crypto throughput	ASA の最大定格 VPN スループット。
Max crypto connections	ASA のサポート対象 VPN トンネルの最大数。
Global Statistics	このセクションは、ASA の複合ハードウェア クリプト アクセラレータに関連しています。

出力（続き）	説明（続き）
Number of active accelerators	アクティブなハードウェア アクセラレータの数。アクティブなハードウェア アクセラレータが初期化されており、crypto コマンドの処理に使用可能です。
Number of non-operational accelerators	非アクティブなハードウェア アクセラレータの数。非アクティブなハードウェア アクセラレータが検出されました。初期化が完了していないか、障害が発生して使用できなくなっています。
Input packets	すべてのハードウェア クリプト アクセラレータで処理される着信パケットの数。
Input bytes	処理される着信パケット内のデータのバイト数。
Output packets	すべてのハードウェア クリプト アクセラレータで処理される発信パケットの数。
Output error packets	エラーが検出された、すべてのハードウェア暗号アクセラレータで処理される発信パケットの数。
Output bytes	処理される発信パケット内のデータのバイト数。
Accelerator 0	各セクションは、クリプト アクセラレータに関連しています。最初のセクション（Accelerator 0）は、常に、ソフトウェア クリプト エンジンです。ハードウェア アクセラレータではありませんが、ASA はこのソフトウェア クリプト エンジンを使用して、特定のクリプト タスクを実行します。ここには、その統計情報が表示されます。Accelerators 1 以上は、常に、ハードウェア クリプト アクセラレータです。
Status（ステータス）	アクセラレータのステータス。アクセラレータが初期化されているか、アクティブか、あるいは失敗したかを示します。
Software crypto engine	アクセラレータのタイプとファームウェア バージョン（該当する場合）。
スロット	アクセラレータのスロット番号（該当する場合）。
Active time	アクセラレータがアクティブ状態であった時間の長さ。
Total crypto transforms	アクセラレータによって実行された crypto コマンドの合計数。
Total dropped packets	エラーのためアクセラレータによってドロップされたパケットの合計数。
Input statistics	このセクションは、アクセラレータで処理された入力トラフィックに関連しています。入力トラフィックは、複合か認証、またはその両方を行う必要がある暗号文と見なされます。
Input packets	アクセラレータによって処理された入力パケットの数。
Input bytes	アクセラレータによって処理された入力バイト数。
Input hashed packets	アクセラレータがハッシュを実行したパケットの数。
Input hashed bytes	アクセラレータがハッシュを実行したバイト数。
Decrypted packets	アクセラレータが対称復号化を実行したパケットの数。
Decrypted bytes	アクセラレータが対称復号化を実行したバイト数。

出力（続き）	説明（続き）
Output statistics	このセクションは、アクセラレータで処理された出力トラフィックに関連しています。入力トラフィックは、暗号化かハッシュ、またはその両方を実行する必要があるクリアテキストと見なされます。
Output packets	アクセラレータによって処理された出力パケットの数。
Output bad packets	エラーが検出された、アクセラレータで処理された出力パケットの数。
Output bytes	アクセラレータによって処理された出力バイト数。
Output hashed packets	アクセラレータが出力ハッシュを実行したパケットの数。
Output hashed bytes	アクセラレータが出力ハッシュを実行したバイト数。
Encyrpted packets	アクセラレータが対称暗号化を実行したパケットの数。
Encyrpted bytes	アクセラレータが対称暗号化を実行したバイト数。
Diffie-Hellman statistics	このセクションは、Diffie-Hellman のキー交換処理に関連しています。
Keys generated	アクセラレータによって生成された Diffie-Hellman キーセットの数。
Secret keys derived	アクセラレータによって生成された Diffie-Hellman 共有秘密の数。
RSA statistics	このセクションは、RSA 暗号処理に関連しています。
Keys generated	アクセラレータによって生成された RSA キー セットの数。
Signatures	アクセラレータによって実行された RSA シグニチャ処理の数。
Verifications	アクセラレータによって実行された RSA シグニチャ確認の数。
Encrypted packets	アクセラレータが RSA 暗号化を実行したパケットの数。
Decrypted packets	アクセラレータが RSA 復号化を実行したパケットの数。
Decrypted bytes	アクセラレータが RSA 復号化を実行したデータのバイト数。
DSA statistics	このセクションは、DSA 処理に関連しています。DSA はバージョン 8.2 以上ではサポートされないため、この統計情報は表示されません。
Keys generated	アクセラレータによって生成された DSA キー セットの数。
Signatures	アクセラレータによって実行された DSA シグニチャ処理の数。
Verifications	アクセラレータによって実行された DSA シグニチャ確認の数。
SSL statistics	このセクションは、SSL レコード処理に関連しています。
Outbound records	アクセラレータによって暗号化され、認証された SSL レコードの数。
Inbound records	アクセラレータによって復号化され、認証された SSL レコードの数。
RNG statistics	このセクションは、乱数生成に関連しています。

出力（続き）	説明（続き）
Random number requests	アクセラレータに対する乱数の要求の数。
Random number request failures	アクセラレータに対する乱数要求のうち、失敗した要求の数。

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

show crypto ca certificates

特定のトラストポイントに関連付けられている証明書、またはシステムにインストールされているすべての証明書を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates [*trustpointname*]

構文の説明

trustpointname	(任意) トラストポイントの名前。名前を指定しない場合は、ASA にインストールされているすべての証明書が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show crypto ca certificates** コマンドの出力例を示します。

```
ciscoasa(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
```

```
        C = US
        EA = example.com
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca aunticate	指定されたトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca enroll	CA を使用して、登録プロセスを開始します。
crypto ca import	指定されたトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定されたトラストポイントでトラストポイント コンフィギュレーション モードを開始します。

show crypto ca crl

キャッシュされているすべての CRL、または指定したトラストポイントでキャッシュされているすべての CRL を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca crl** コマンドを使用します。

show crypto ca crl [trustpool | trustpoint <*trustpointname*>**]**

構文の説明

trustpoint *trustpointname*	（任意）トラストポイントの名前。名前を指定しない場合は、ASA にキャッシュされているすべての CRL が表示されます。
trustpool	trustpool の名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show crypto ca crl** コマンドの出力例を示します。

```
ciscoasa(config)# show crypto ca crl tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca aunticate	指定されたトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca enroll	CA を使用して、登録プロセスを開始します。
crypto ca import	指定されたトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定されたトラストポイントでトラストポイント コンフィギュレーション モードを開始します。

show crypto ca server

ASA でローカル CA コンフィギュレーションのステータスを表示するには、CA サーバ コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server** コマンドを使用します。

show crypto ca server

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、**show crypto ca server** コマンドの出力例を示します。

```
ciscoasa# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
    Status: disabled
    State: disabled
    Server's configuration is unlocked (enter "no shutdown" to lock it)
    Issuer name: CN=asa1.cisco.com
    CA cert fingerprint: -Not found-
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 2009
    CRL not present.
    Current primary storage dir: nvram:
ciscoasa#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
debug crypto ca server	ローカル CA サーバを設定するときに、デバッグ メッセージを表示します。
show crypto ca server certificate	ローカル CA の証明書を Base-64 形式で表示します。
show crypto ca server crl	ローカル CA CRL のライフタイムを表示します。

show crypto ca server cert-db

ローカル CA サーバ証明書の全部またはサブセット(特定のユーザに発行されたものも含む)を表示するには、CA サーバ コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server cert-db** コマンドを使用します。

show crypto ca server cert-db [**username** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]

構文の説明

allowed	証明書のステータスに関係なく、登録を許可されたユーザを表示するように指定します。
enrolled	有効な証明書を持つユーザを表示するように指定します。
expired	期限切れの証明書を保持しているユーザを表示するように指定します。
on-hold	まだ登録されていないユーザを表示するように指定します。
serial *certificate-serial-number*	表示する特定の証明書のシリアル番号を指定します。シリアル番号は 16 進形式である必要があります。
username *username*	証明書の所有者を指定します。username は、ユーザ名または電子メール アドレスです。電子メール アドレスの場合、エンド ユーザに連絡を取りワンタイム パスワード(OTP)を配布するために使用される電子メール アドレスになります。エンド ユーザの電子メール通知をイネーブルにするには、電子メール アドレスが必要です。

デフォルト

デフォルトでは、ユーザ名も証明書シリアル番号も指定されていない場合、発行された証明書のデータベース全体が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

show crypto ca server cert-db コマンドは、ローカル CA サーバによって発行されたユーザ証明書のリストを表示します。1 つ以上の任意の証明書タイプ キーワードを付けて、または任意の証明書シリアル番号を付けて、特定のユーザ名を指定することで、証明書データベースのサブセットを表示できます。

キーワードまたはシリアル番号なしでユーザ名を指定すると、そのユーザに対して発行された証明書がすべて表示されます。ユーザごとに、出力には、ユーザ名、電子メール アドレス、ドメイン名、登録が許可される期間、およびユーザに登録招待が通知された回数が表示されます。

また、出力には次の情報も表示されます。

- NOTIFIED フィールドは、複数のリマインダをサポートするために必要です。これにより、登録およびリマインダ通知を試行するためにユーザに OTP の通知を行う必要があるタイミングが追跡されます。このフィールドは、最初は 0 に設定されています。ユーザ入力に登録許可のマークが付くと、このフィールドは増分して 1 になります。この時点で、最初の OTP 通知が生成されます。
- NOTIFY フィールドは、リマインダが送信されるたびに増分します。OTP が期限切れになるまでに 3 つの通知が送信されます。ユーザが登録を許可されたとき、有効期間の中間点、および有効期間の 3/4 を経過した時点で通知が送信されます。このフィールドは、管理者が開始した登録でのみ使用されます。自動証明書更新の場合、証明書データベース内の NOTIFY フィールドが使用されます。

(注) 有効期限前に証明書の更新がユーザに通知される回数を追跡する場合にはこのコマンドの通知カウンタが使用され、証明書の登録がユーザに通知される回数を追跡する場合には show crypto ca server user-db の通知カウンタが使用されます。更新通知は、cert-db で追跡され、user-db には含まれません。

それぞれの証明書には、証明書のシリアル番号、発行日付と有効期限日付、および証明書のステータス（Revoked/Not Revoked）が表示されます。

例

次に、CA サーバが ASA に対して発行した証明書をすべて表示するよう要求する例を示します。

```
ciscoasa# show crypto ca server cert-db username asa
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

次に、ローカル CA サーバによって発行された、シリアル番号が 0x2 の証明書をすべて表示するよう要求する例を示します。

```
ciscoasa# show crypto ca server cert-db serial 2

Username:asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

次に、ローカル CA サーバによって発行された証明書をすべて表示するよう要求する例を示します。

```
ciscoasa# show crypto ca server cert-db
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL の両方で失効としてマークします。
lifetime crl	CRL のライフタイムを指定します。

show crypto ca server certificate

ローカル CA サーバの証明書を Base-64 形式で表示するには、CA サーバ コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server certificate** コマンドを使用します。

show crypto ca server certificate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

show crypto ca server certificate コマンドにより、ローカル CA サーバの証明書が Base-64 形式で表示されます。この表示画面では、ローカル CA サーバを信頼する必要がある他のデバイスに証明書をエクスポートするときに、その証明書をカット アンド ペーストできます。

例

次に、**show crypto ca server certificate** コマンドの出力例を示します。

```
ciscoasa# show crypto ca server certificate

The base64 encoded local CA certificate follows:

MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+
MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAM
IIXHAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQ
Ijph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphs
UM+IG3SDOiDwZG9n1SvtMieoxd7Hxknxbum06JDruj
```

```
WKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzw
cRhl1KEZTS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeL
j3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwP
EdPQxaWZPrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3
Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d
5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI0b2AfCr6Pbw
fC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA
5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3qAXy1
GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

ciscoasa#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。
ライフタイム	CA 証明書と発行済みの証明書のライフタイムを指定します。
show crypto ca server	ローカル CA コンフィギュレーションを ASCII テキスト形式で表示します。

show crypto ca server crl

ローカル CA の現在の CRL を表示するには、CA サーバ コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server crl** コマンドを使用します。

show crypto ca server crl

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、**show crypto ca server crl** コマンドの出力例を示します。

```
ciscoasa# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
    Issuer: cn=asa5540.frqa.cisco.com
    This Update: 07:32:27 UTC Oct 16 2006
    Next Update: 13:32:27 UTC Oct 16 2006
    Number of CRL entries: 0
    CRL size: 232 bytes
asa5540(config)#
ciscoasa#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める CRL 分散ポイント(CDP)を指定します。
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
lifetime crl	CRL のライフタイムを指定します。
show crypto ca server	CA コンフィギュレーションのステータスを表示します。

show crypto ca server user-db

ローカル CA サーバのユーザ データベースに含まれているユーザを表示するには、CA サーバ コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server user-db** コマンドを使用します。

show crypto ca server user-db [**expired** | **allowed** | **on-hold** | **enrolled**]

構文の説明

allowed	(任意)証明書のステータスに関係なく、登録を許可されたユーザを表示するように指定します。
enrolled	(任意)有効な証明書を持つユーザを表示するように指定します。
expired	(任意)期限切れの証明書を保持しているユーザを表示するように指定します。
on-hold	(任意)まだ登録されていないユーザを表示するように指定します。

デフォルト

デフォルトでは、キーワードが入力されない場合にはデータベース内のすべてのユーザが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、現在登録されているユーザを表示する例を示します。

```
ciscoasa# show crypto ca server user-db enrolled
Username    DN                  Certificate issued    Certificate expiration
exampleusercn=Example User,o=...5/31/2009           5/31/2010

ciscoasa#
```

使用上のガイドライン

証明書の登録がユーザに通知される回数を追跡する場合にはこのコマンドの通知カウンタが使用され、有効期限前に証明書の更新がユーザに通知される回数を追跡する場合には show crypto ca server cert-db の通知カウンタが使用されます。更新通知は、cert-db で追跡され、user-db には含まれません。

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、ローカル CA への登録を許可します。
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
crypto ca server user-db write	ローカル CA データベースで設定されているユーザ情報をストレージに書き込みます。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

show crypto ca trustpool

trustpool を構成する証明書を表示するには、特権 EXEC モードで **show crypto ca trustpool** コマンドを使用します。

show crypto ca trustpool [detail]

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、すべての trustpool を省略形式で表示します。「detail」オプションを指定した場合は、追加の情報が含まれます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show crypto ca trustpool コマンドの出力には、各証明書のフィンガープリントの値が含まれます。これらの値は削除操作で必要です。

例

```
ciscoasa# show crypto ca trustpool

CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bxb2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
Validity Date:
```

```
start date:17:21:06 EST Jan 14 2009
end date:17:31:06 EST Jan 14 2024

CA Certificate
Status: Available
Certificate Serial Number: 58d1c756000000000059
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bxb2008-root
dc=bxb2008
dc=mycompany
dc=com
Subject Name:
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bxb2008-1.bxb2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bxb2008-1.bxb2008.mycompany.com/CertEnroll/bxb2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011
```

関連コマンド

コマンド	説明
clear crypto ca trustpool	trustpool からすべての証明書を削除します。
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。
crypto ca trustpool remove	指定された 1 つの証明書を trustpool から削除します。

show crypto ca trustpool policy

設定済みの trustpool ポリシーを表示し、適用された証明書マップを処理してそれらがポリシーに与える影響を表示するには、特権 EXEC モードで **show crypto ca trustpool policy** コマンドを使用します。

show crypto ca trustpool policy

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.5(2)	trustpool 証明書の自動インポートのステータスと結果を表示する機能が追加されました。

例

```
ciscoasa(config)# sh run cry ca cert map
crypto ca certificate map map1 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca
crypto ca certificate map map 2 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca2
ciscoasa(config)#

ciscoasa(config)# sh run crypto ca trustpool policy
crypto ca trustpool policy
auto-import url http://www.thawte.com
revocation-check none
match certificate map2 allow expired-certificate
match certificate map1 skip revocation-check
crl cache-time 123
crl enforcenextupdate
auto-import
auto-import url http://www.thawte.com
auto-import time 22:00:00
```

```
ciscoasa(config)#

ciscoasa# show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool auto import statistics:
    Last import result: SUCCESS
    Next scheduled import at 22:00:00 Tues Jul 21 2015
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.thawte.com
Download time: 22:00:00
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
action:skip revocation-check

map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates

ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpool policy	トラストプール ポリシーを定義するコマンドを提供するサブモードを開始します。

show crypto debug-condition

IPsec および ISAKMP のデバッグ メッセージに対して現在設定されているフィルタ、一致しない状態、およびエラー状態を表示するには、グローバル コンフィギュレーション モードで **show crypto debug-condition** コマンドを使用します。

show crypto debug-condition

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、フィルタリング条件を表示する例を示します。

```
ciscoasa(config)# show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPsec debug context unmatched flag:  ON

IKE peer IP address filters:
1.1.1.0/24   2.2.2.2

IKE user name filters:
my_user
```

関連コマンド

コマンド	説明
debug crypto condition	IPsec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。
debug crypto condition error	フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。
debug crypto condition unmatched	フィルタリングに十分なコンテキスト情報が含まれていない IPsec および ISAKMP のデバッグ メッセージを表示します。

show crypto ikev1 sa

IKEv1 ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ikev1 sa** コマンドを使用します。

show crypto ikev1 sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE Peer	タイプ	Dir	Rky	状態
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE Peer	タイプ	Dir	Rky	状態	Encrypt	Hash	認証	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
ciscoasa(config)# show crypto ikev1 sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

関連コマンド

コマンド	説明
show crypto ikev2 sa	IKEv2 ランタイム SA データベースを表示します。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ikev2 sa

IKEv2 ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ikev2 sa** コマンドを使用します。

show crypto ikev2 sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE Peer	タイプ	Dir	Rky	状態
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE Peer	タイプ	Dir	Rky	状態	Encrypt	Hash	認証	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
ciscoasa(config)# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
671069399                10.0.0.0/500 10.255.255.255/500      READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/188 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 80173A0373C2D403       Remote spi: AE8AEFA1B97DBB22
      Local id: asa
      Remote id: asa1
      Local req mess id: 8              Remote req mess id: 7
      Local next mess id: 8             Remote next mess id: 7
      Local req queued: 8               Remote req queued: 7
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x242a3da5/0xe6262034
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

関連コマンド

コマンド	説明
show crypto ikev1 sa	IKEv1 ランタイム SA データベースを表示します。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ikev2 stats

IKEv2 の実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ikev2 stats** コマンドを使用します。

show crypto ikev2 stats]

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.9(1)	ローカル IKEv2 の統計情報が提供されるようになりました。

使用上のガイドライン

このコマンドのローカルの出力は次のとおりです。

```
Local IKEv2 Statistics
Active Tunnels: 320
Previous Tunnels: 1244
In Octets: 4133968
In Packets: 40527
In Drop Packets: 0
In Drop Fragments: 0
```

関連コマンド

コマンド	説明
show crypto ikev2 sa	IKEv1 ランタイム SA データベースを表示します。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ipsec df-bit

指定されたインターフェイスの IPsec パケットの IPsec do-not-fragment（DF ビット）ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec df-bit** コマンドを使用します。また、同じ意味を持つ **show ipsec df-bit** コマンドも使用できます。

show crypto ipsec df-bit *interface*

構文の説明

interface	インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

df ビットの設定によって、カプセル化されたヘッダーの do-not-fragment（DF）ビットのシステムによる処理方法が決まります。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。この設定に基づき、システムは暗号の適用時に外側の IPsec ヘッダーに対するクリアテキスト パケットの DF ビットの設定をクリアするか、設定するか、コピーするかのいずれかを実行します。

例

次に、inside というインターフェイスの IPsec DF ビット ポリシーを表示する例を示します。

```
ciscoasa(config)# show crypto ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPsec パケットの IPsec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPsec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec fragmentation** コマンドを使用します。また、同じ意味を持つ **show ipsec fragmentation** コマンドも使用できます。

show crypto ipsec fragmentation *interface*

構文の説明

interface	インターフェイス名を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

VPN に対するパケットを暗号化する際、システムはパケット長をアウトバウンド インターフェイスの MTU と比較します。パケットの暗号化が MTU を超える場合は、パケットをフラグメント化する必要があります。このコマンドは、パケットを暗号化した後（after-encryption）、または暗号化する前（before-encryption）にシステムがパケットをフラグメント化するかどうかを表示します。暗号化前のパケットのフラグメント化は、事前フラグメント化とも呼ばれ、暗号化パフォーマンス全体を向上させるため、システムのデフォルト動作になっています。

例

次に、グローバル コンフィギュレーション モードで、inside という名前のインターフェイスの IPsec フラグメンテーション ポリシーを表示する例を示します。

```
ciscoasa(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPsec パケットの DF ビット ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show crypto ipsec policy

OSPFv3 に設定されている IPsec セキュア ソケット API（SS API）セキュリティ ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec policy** コマンドを使用します。このコマンドの別の形式である **show ipsec policy** を使用することもできます。

show crypto ipsec policy

構文の説明

このコマンドには、キーワードや変数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、OSPFv3 認証と暗号方式ポリシーを表示する例を示します。

```
ciscoasa# show crypto ipsec policy

Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901234567890
Outbound ESP Auth Key:   12345678901234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

関連コマンド

コマンド	説明
ipv6 ospf encryption	OSPFv3 の認証と暗号方式ポリシーを設定します。
show crypto sockets	セキュアなソケット情報を表示します。
show ipv6 ospf interface	OSPFv3 インターフェイスに関する情報を表示します。

show crypto ipsec sa

IPsec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec sa** コマンドを使用します。このコマンドの別の形式である **show ipsec sa** を使用することもできます。

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

構文の説明

detail	(任意)表示されているものに対する詳細なエラー情報を表示します。
entry	(オプション)IPsec SA をピア アドレスの順に表示します。
identity	(オプション)IPsec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
map *map-name*	(オプション)指定されたクリプト マップの IPsec SA を表示します。
peer *peer-addr*	(オプション)指定されたピア IP アドレスの IPsec SA を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	OSPFv3、マルチ コンテキスト モード、トランスフォームと IV サイズ部分における Suite B アルゴリズム、および ESPV3 IPsec 出力に対するサポートが追加されました。
9.13(1)	***show crypto ipsec sa detail*** で発生するエラーのトラブルシューティング用として、次の新しいカウンタが追加されました。 • ***#pkts invalid ip version (send)*** • ***#pkts invalid length (send)*** • ***#pkts invalid ctx (send) and #pkts invalid ctx (rcv)*** • ***#pkts invalid ifc (send) and #pkts invalid ifc (rcv)*** • ***#pkts failed (send) and #pkts failed (rcv)***

例

次に、グローバル コンフィギュレーション モードで、OSPFv3 として識別されるトンネルを含む IPsec SA を表示する例を示します。

```
ciscoasa(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

(注) IPSec SA ポリシーに、フラグメンテーションは IPsec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーに、フラグメンテーションは IPsec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

グローバル コンフィギュレーション モードで入力された次の例に、トラフィックエラーのトラブルシューティング用として新しく追加されたカウンタを使用して、キーワード detail の IPsec SA を示します。

```
(config)# sh ipsec sa det
interface: outside
    Crypto map tag: outside_map, seq num: 10, local addr: 10.86.94.103

      access-list toASA-5525 extended permit ip host 10.86.94.103 host 10.86.95.135
```

```
  local ident (addr/mask/prot/port): (10.86.94.103/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.86.95.135/255.255.255.255/0/0)
  current_peer: 10.86.95.135

  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
  #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0
  #pkts invalid pad (rcv): 0

  #pkts invalid ip version (send): 0, #pkts invalid ip version (rcv): 0
  #pkts invalid len (send): 0, #pkts invalid len (rcv): 0
  #pkts invalid ctx (send): 0, #pkts invalid ctx (rcv): 0
  #pkts invalid ifc (send): 0, #pkts invalid ifc (rcv): 0
  #pkts failed (send): 0, #pkts failed (rcv): 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

  local crypto endpt.: 10.86.94.103/500, remote crypto endpt.: 10.86.95.135/500
  path mtu 1500, ipsec overhead 94(44), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: 25356578
  current inbound spi : A1029CE2

inbound esp sas:
  spi: 0xA1029CE2 (2701303010)
     SA State: active
     transform: esp-aes esp-sha-512-hmac no compression
     in use settings ={L2L, Tunnel, IKEv2, }
     slot: 0, conn_id: 195272704, crypto-map: outside_map
     sa timing: remaining key lifetime (kB/sec): (3962879/28782)
     IV size: 16 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x0000001F

outbound esp sas:
  spi: 0x25356578 (624256376)
     SA State: active
     transform: esp-aes esp-sha-512-hmac no compression
     in use settings ={L2L, Tunnel, IKEv2, }
     slot: 0, conn_id: 195272704, crypto-map: outside_map
     sa timing: remaining key lifetime (kB/sec): (4193279/28772)
     IV size: 16 bytes
     replay detection support: Y
     Anti replay bitmap:
   0x00000000 0x00000001
```

次に、グローバル コンフィギュレーション モードで、def という名前のクリプト マップの IPsec SA を表示する例を示します。

```
ciscoasa(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
```

```
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 4, crypto-map: def
        sa timing: remaining key lifetime (sec): 263
        IV size: 8 bytes
        replay detection support: Y
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry** に対する IPsec SA を表示する例を示します。

```
ciscoasa(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 3, crypto-map: def
        sa timing: remaining key lifetime (sec): 429
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 3, crypto-map: def
        sa timing: remaining key lifetime (sec): 429
        IV size: 8 bytes
        replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
```

```
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry detail** を使用して IPsec SA を表示する例を示します。

```
ciscoasa(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

次に、キーワード **identity** を使用した IPsec SA の例を示します。

```
ciscoasa(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
```

```
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次に、キーワード **identity** および **detail** を使用した IPsec SA の例を示します。

```
ciscoasa(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
```

```
#pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
#pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35
```

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ipsec stats

IPsec 統計情報のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec stats** コマンドを使用します。

show crypto ipsec stats

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
ciscoasa(config)# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
```

```
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	指定されたパラメータに基づいて、IPsec SA またはカウンタをクリアします。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定されたパラメータに基づいて IPsec SA を表示します。
show ipsec sa summary	IPsec SA の要約を表示します。

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
```

```
No Sa Fails: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp sa** コマンドを使用します。

show crypto isakmp sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが追加されました。
7.2(1)	この **show isakmp sa** コマンドは廃止されました。**show crypto isakmp sa** コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE Peer：209.165.200.225

Type：L2L または User

Dir：Init

Rky：No または Yes。Yes の場合は、キー再生成が発生しており、キー再生成が完了するまで、2 番目に一致する SA は異なる状態になります。

Role：Initiator または Responder State。SA のステート マシンの現在の状態を示します。

State：トンネルがアップしデータが受け渡しされている場合、値は MM_ACTIVE または AM_ACTIVE のいずれかになります。その他のアクティブ状態は、MM_BLD_MSG4、MM_BLD_MSG6、MM_FREE、MM_SND_MSG6_H、MM_START、MM_TM_INIT_MODECFG_H、MM_TM_PEND_QM、MM_WAIT_DELETE、MM_WAIT_MSG3、MM_WAIT_MSG5 などです。

detail オプションを指定した場合

IKE Peer：209.165.200.225

Type：L2L または User

Dir：Init

Rky：No または Yes。Yes の場合は、キー再生成が発生しており、キー再生成が完了するまで、2 番目に一致する SA は異なる状態になります。

Role：Initiator または Responder State。SA のステート マシンの現在の状態を示します。トンネルがアップしデータが受け渡しされている場合、値は MM_ACTIVE または AM_ACTIVE のいずれかになります。

State：MM_ACTIVE または AM_ACTIVE 以外。その他のアクティブ状態は、MM_BLD_MSG4、MM_BLD_MSG6、MM_FREE、MM_SND_MSG6_H、MM_START、MM_TM_INIT_MODECFG_H、MM_TM_PEND_QM、MM_WAIT_DELETE、MM_WAIT_MSG3、MM_WAIT_MSG5 などです。

Encrypt：3des

Hash：md5

Auth：preshrd

Lifetime：86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
ciscoasa(config)# show crypto isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp stats

実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが追加されました。
7.2(1)	**show isakmp stats** コマンドが非推奨コマンドになりました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests

- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto key mypubkey

ECDSA キーのキー名、使用方法、および楕円曲線サイズを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto key mypubkey** コマンドを使用します。

show crypto key mypubkey dsa | rsa

構文の説明

dsa	キー名を指定します。
rsa	キー名を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

show crypto protocol statistics

クリプト アクセラレータ MIB 内のプロトコル固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto protocol statistics** コマンドを使用します。

show crypto protocol statistics *protocol*

構文の説明

protocol	統計情報を表示するプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。 **ikev1**：インターネット キー交換バージョン 1。 **ipsec**：IP セキュリティ フェーズ 2 プロトコル。 **ssl**：Secure Sockets Layer（SSL） **other**：新規プロトコル用に予約済み。 **all**：現在サポートされているすべてのプロトコル。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードで、指定したプロトコルに関するクリプト アクセラレータ統計情報を表示する例を示します。

```
ciscoasa # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
```

```
   SA rekey requests: 3
    SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0

ciscoasa # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

ciscoasa # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

ciscoasa # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

ciscoasa # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
```

```
    Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 0
    Failed requests: 0
[IPsec statistics]
    Encrypt packet requests: 700
    Encapsulate packet requests: 700
    Decrypt packet requests: 700
    Decapsulate packet requests: 700
    HMAC calculation requests: 1400
    SA creation requests: 2
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 0
    Failed requests: 0
[SSL statistics]
    Encrypt packet requests: 0
    Encapsulate packet requests: 0
    Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 0
    Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
    Encrypt packet requests: 0
    Encapsulate packet requests: 0
    Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 99
    Failed requests: 0
ciscoasa #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。

show crypto sockets

暗号セキュア ソケット情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto sockets** コマンドを使用します。

show crypto sockets

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードで、暗号セキュア ソケット情報を表示する例を示します。

```
ciscoasa(config)# show crypto sockets

Number of Crypto Socket connections 1

       Gi0/1  Peers: (local): 2001:1::1
                     (remote): ::
              Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
              Remote Ident (addr/plen/port/prot): (::/0/0/89)
              IPsec Profile: "CSSU-UTF"
              Socket State: Open
              Client: "CSSU_App(UTF)" (Client State: Active)

       Crypto Sockets in Listen state:
```

次の表に、**show crypto sockets** コマンドの出力のフィールドを示します。

フィールド	説明
Number of Crypto Socket connections	システム内の暗号ソケットの数。
Socket State	この状態は、アクティブな IPsec セキュリティ アソシエーション（SA）が存在することを意味する Open か、またはアクティブな IPsec SA が存在しないことを意味する Closed のどちらかです。
クライアント	アプリケーションの名前とその状態。
Flags	このフィールドが「shared」になっている場合、ソケットは複数のトンネル インターフェイスで共有されます。
Crypto Sockets in Listen state	暗号 IPsec プロファイルの名前。

関連コマンド

コマンド	説明
show crypto ipsec policy	暗号セキュア ソケット API でインストールされたポリシー情報を表示します。

show csc node-count

CSC SSM がスキャンしたトラフィックのノード数を表示するには、特権 EXEC モードで **show csc node-count** コマンドを使用します。

show csc node-count [**yesterday**]

構文の説明

yesterday	（任意）CSC SSM が前日の 24 時間（午前 0 時から翌日の午前 0 時まで）スキャンしたトラフィックのノード数を表示します。

デフォルト

デフォルトで表示されるノード カウントは、午前 0 時からスキャンされたノード数です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ノードとは、固有の送信元 IP アドレス、または ASA により保護されているネットワーク上のデバイスのアドレスです。ASA は、毎日のノード カウントを追跡し、ユーザ ライセンスの強制のために CSC SSM に伝えます。

例

次に、CSC SSM が午前 0 時以降にスキャンしたノードの数を表示する **show csc node-count** コマンドの出力例を示します。

```
ciscoasa# show csc node-count
Current node count is 1
```

次に、CSC SSM が過去 24 時間（午前 0 時から翌日の午前 0 時まで）にスキャンしたトラフィックのノード数を表示する **show csc node-count** コマンドの出力例を示します。

```
ciscoasa(config)# show csc node-count yesterday
Yesterday's node count is 2
```

関連コマンド

csc	ネットワーク トラフィックを CSC SSM に送信して、CSC SSM で設定されているとおりに FTP、HTTP、POP3、および SMTP をスキャンします。
show running-config class-map	現在のクラス マップ コンフィギュレーションを表示します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションを表示します。
show running-config service-policy	現在のサービス ポリシー コンフィギュレーションを表示します。

show ctiqbe

ASA を越えて確立された CTIQBE セッションの情報を表示するには、特権 EXEC モードで **show ctiqbe** コマンドを使用します。

show ctiqbe

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show ctiqbe コマンドは、ASA を越えて確立された CTIQBE セッションの情報を表示します。**debug ctiqbe** や **show local-host** とともに、このコマンドは、CTIQBE インスペクション エンジンの問題のトラブルシューティングに使用されます。

(注) **show ctiqbe** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの CTIQBE セッションが存在し、**pager** コマンドが設定されていない場合、**show ctiqbe** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例

次の条件における **show ctiqbe** コマンドの出力例を示します。ASA を越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco CallManager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
ciscoasa# | show ctiqbe

Total: 1
        LOCAL           FOREIGN         STATE   HEARTBEAT
-------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
```

```
-----------------------------------------
RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
-----------------------------------------
MEDIA: Device ID 27     Call ID 0
       Foreign 172.29.1.99      (1028 - 1029)
       Local   172.29.1.88      (26822 - 26823)
-----------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスおよび RTP 受信ポートは 172.29.1.99 の UDP ポート 1028 に PAT 変換されています。RTCP 受信ポートは UDP 1029 に PAT 変換されています。

`RTP/RTCP: PAT xlates:` で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートがその外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに NAT 変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP 受信ポートは、UDP 26822 および 26823 です。ASA は 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話機は、CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レッグは、Device ID 27 および Call ID 0 で確認できます。

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション インスペクションをイネーブルにします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show ctl-file

電話プロキシで使用される CTL ファイルの内容を表示するには、グローバル コンフィギュレーション モードで **show ctl-file** コマンドを使用します。

show ctl-file *filename* [**parsed**]

構文の説明

filename	データベースに格納されているセキュア モードに対応した電話を表示します。
parsed	（任意）指定した CTL ファイルの詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	コマンドが追加されました。

使用上のガイドライン

フラッシュ メモリに格納されている CTL ファイルのファイル名を指定する場合は、ディスク番号、ファイル名、および拡張を `disk0:/testctl.tlv` のように指定します。**show ctl-file** コマンドを使用すると、電話プロキシ インスタンスの設定時のデバッグに役立ちます。

例

次に、**show ctl-file** コマンドを使用して、CTL ファイルの一般情報を表示する例を示します。

```
ciscoasa# show ctl-file disk0:/ctlfile.tlv
Total Number of Records: 1
CTL Record Number 1
  Subject Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Issuer Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Function:
     cucm
  IP Address:
     192.168.52.102
  Associated Trustpoint:
     cucm_primary
```

次に、**show ctl-file** コマンドを使用して、CTL ファイルの詳細情報を表示する例を示します。

```
ciscoasa# show ctl-file disk0:/ctlfile.tlv parsed
TAG 0x01: Version: Maj 1, Min 2
TAG 0x02: Header Len: Len 288
TAG 0x03: Signer ID: Len 103
TAG 0x04: Signer Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x05: Cert SN: Len 4 SN: c43c9048
TAG 0x06: CA Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x07: Signature: Len 15
TAG 0x08: Digest Alg: Len 1 Name: SHA-1
TAG 0x09: Sig Alg Info: Len 8
TAG 0x0A: Sig Alg: Len 1 Name: RSA
TAG 0x0B: Modulus: Len 1 Name: 1024
TAG 0x0C: Sig Block: Len 128 Signature:
    521debcf b7a77ea8 94eba5f7 f3c8b0d8 3337a9fa 267ce1a7 202b2c8b 2ac980d3
    9608f64d e7cd82df e205e5bf 74a1d9c4 fae20f90 f3d2746a e90f439e ef93fca7
    d4925551 72daa414 2c55f249 ef7e6dc2 bcb9f9b5 39be8238 5011eecb ce37e4d1
    866e6550 6779c3fd 25c8bab0 6e9be32c 7f79fe34 5575e3af ea039145 45ce3158

TAG 0x0E: File Name: Len 12 Name: <CTLFile.tlv>
TAG 0x0F: Timestamp: Len 4 Timestamp: 48903cc6

 ### CTL RECORD No. 1 ###
TAG 0x01: Rcd Len: Len 731
TAG 0x03: Sub Name: Len 43 Sub Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x04: Function: Len 2 Func: CCM
TAG 0x05: Cert Issuer: Len 43 Issuer Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x06: Cert SN: Len 4 Cert SN: 15379048
TAG 0x07: Pub Key: Len 140 Pub Key:
    30818902 818100ad a752b4e6 89769a49 13115e52 1209b3ef 96a179af 728c29d7
    af7fed4e c759d0ea cebd7587 dd4f7c4c 322da86b 3a677c08 ce39ce60 2525f6d2
    50fe87cf 2aea60a5 690ec985 10706e5a 30ad26db e6fdb243 159758ed bb487525
    f901ef4a 658445de 29981546 3867d2d1 ce519ee4 62c7be32 51037c3c 751c0ad6
    040bedbb 3e984502 03010001
TAG 0x09: Cert: Len 469 X.509v3 Cert:
    308201d1 3082013a a0030201 02020415 37904830 0d06092a 864886f7 0d010104
    0500302d 312b3012 06035504 05130b4a 4d583132 31354c32 54583015 06092a86
    4886f70d 01090216 08636973 636f6173 61301e17 0d303830 37333030 39343033
    375a170d 31383037 32383039 34303337 5a302d31 2b301206 03550405 130b4a4d
    58313231 354c3254 58301506 092a8648 86f70d01 09021608 63697363 6f617361
    30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ada752
    b4e68976 9a491311 5e521209 b3ef96a1 79af728c 29d7af7f ed4ec759 d0eacebd
    7587dd4f 7c4c322d a86b3a67 7c08ce39 ce602525 f6d250fe 87cf2aea 60a5690e
    c9851070 6e5a30ad 26dbe6fd b2431597 58edbb48 7525f901 ef4a6584 45de2998
    15463867 d2d1ce51 9ee462c7 be325103 7c3c751c 0ad6040b edbb3e98 45020301
    0001300d 06092a86 4886f70d 01010405 00038181 005d82b7 ac45dbf8 bd911d4d
    a330454a a2784a4b 5ef898b1 482e0bbf 4a86ed86 9019820b 00e80361 fd7b2518
    9efa746c b98b1e23 fcc0793c de48de6d 6b1a4998 cd6f4e66 ba661d3a d200739a
    ae679c7c 94f550fb a6381b94 1eae389e a9ec4b11 30ba31f3 33cd184e 25647174
    ce00231d 102d5db3 c9c111a6 df37eb43 66f3d2d5 46
TAG 0x0A: IP Addr: Len 4 IP Addr: 192.168.52.102
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	電話プロキシを作成するための CTL インスタンスを指定するか、またはフラッシュ メモリに格納されている CTL ファイルを解析します。
ctl-file（**Phone-Proxy**）	電話プロキシの設定時に使用する CTL インスタンスを指定します。
phone proxy	Phone Proxy インスタンスを設定します。

show ctl-provider

ユニファイド コミュニケーションで使用される CTL プロバイダーの設定を表示するには、特権 EXEC モードで **show CTL provider** コマンドを使用します。

show ctl-provider [*name*]

構文の説明

name	（オプション）この CTL プロバイダーのみの情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、CTL プロバイダーの設定を表示する例を示します。

```
ciscoasa# show ctl-provider
!
ctl-provider my-ctl
 client interface inside address 192.168.1.55
 client interface inside address 192.168.1.56
 client username admin password gWe.oMSKmeGtelxS encrypted
 export certificate ccm-proxy
!
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダーを設定します。

show cts environment-data

ASA に Cisco TrustSec の環境データのリフレッシュ処理のヘルス状態とステータスを表示するには、特権 EXEC モードで **show cts environment-data** コマンドを使用します。

show cts environment-data

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、フェールオーバー コンフィギュレーションのスタンバイ状態のデバイスではサポートされません。スタンバイ状態のデバイスでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
ERROR: This command is only permitted on the active device.
```

このコマンドは、クラスタリング コンフィギュレーションのマスター ユニットでのみサポートされます。スレーブ ユニットでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
This command is only permitted on the master device.
```

例

次に、**show cts environment-data** コマンドの出力例を示します。

```
ciscoasa# show cts environment-data

CTS Environment Data
====================
Status:                  Active
Last download attempt:   Successful
Environment Data Lifetime: 1200 secs
Last update time:        18:12:07 EST Feb 27 2012
```

```
Env-data expires in:        0:00:12:24 (dd:hr:mm:sec)
Env-data refreshes in:      0:00:02:24 (dd:hr:mm:sec)
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts pac	PAC のコンポーネントを表示します。

show cts environment-data sg-table

ASA に Cisco TrustSec の常駐セキュリティ グループ テーブルを表示するには、特権 EXEC モードで **show cts environment-data sg-table** コマンドを使用します。

show cts environment-data sg-table

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、フェールオーバー コンフィギュレーションのスタンバイ状態のデバイスではサポートされません。スタンバイ状態のデバイスでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
ERROR: This command is only permitted on the active device.
```

このコマンドは、クラスタリング コンフィギュレーションのマスター ユニットでのみサポートされます。スレーブ ユニットでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
This command is only permitted on the master device.
```

例

次に、**show cts environment-data sg-table** コマンドの出力例を示します。

```
ciscoasa# show cts environment-data sg-table

Security Group Table:
Valid until: 18:32:07 EST Feb 27 2012
Showing 9 of 9 entries

SG Name                         SG Tag     Type
-------                         ------     -------------
```

```
ANY                                 65535     unicast
ExampleSG1                              2     unicast
ExampleSG13                            14     unicast
ExampleSG14                            15     unicast
ExampleSG15                            16     unicast
ExampleSG16                            17     unicast
ExampleSG17                            18     unicast
ExampleSG18                            19     unicast
Unknown                                 0     unicast
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts pac	PAC のコンポーネントを表示します。

show cts pac

ASA に Cisco TrustSec の Protected Access Credential（PAC）のコンポーネントを表示するには、特権 EXEC モードで **show cts pac** コマンドを使用します。

show cts pac

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show cts pac コマンドは、PAC 情報（有効期間など）を表示します。PAC のライフタイムが経過すると ASA がセキュリティ グループ テーブルの更新を取得できなくなるため、有効期間は重要です。管理者は、Identity Services Engine のセキュリティ グループ テーブルとの同期を保つために、古い PAC の期限が切れる前に新しい PAC を要求する必要があります。

このコマンドは、フェールオーバー コンフィギュレーションのスタンバイ状態のデバイスではサポートされません。スタンバイ状態のデバイスでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
ERROR: This command is only permitted on the active device.
```

このコマンドは、クラスタリング コンフィギュレーションのマスター ユニットでのみサポートされます。スレーブ ユニットでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
This command is only permitted on the master device.
```

例

次に、**show cts pac** コマンドの出力例を示します。

```
ciscoasa# show cts pac
PAC-Info:
    Valid until: Jul 28 2012 08:03:23
    AID:         6499578bc0240a3d8bd6591127ab270c
    I-ID:        BrianASA36
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200b000030001000400106499578bc0240a3d8bd6591127ab270c00060094000301
    00d75a3f2293ff3b1310803b9967540ff7000000134e2d2deb00093a803d227383e2b9
    7db59ed2eeac4e469fcb1eeb0ac2dd84e76e13342a4c2f1081c06d493e192616d43611
    8ff93d2af9b9135bb95127e8b9989db36cf1667b4fe6c284e220c11e1f7dbab91721d1
    00e9f47231078288dab83a342ce176ed2410f1249780882a147cc087942f52238fc9b4
    09100e1758
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show cts sgt-map

制御パスの IP アドレス セキュリティ グループ テーブル マネージャ エントリを表示するには、特権 EXEC モードで **show cts sgt-map** コマンドを使用します。

show cts sgt-map [**sgt** *sgt*] [**address** *ipv4*[*/mask*] | **address** *ipv6* [*/prefix*] | **ipv4** | **ipv6**] [**name**] [**brief** | **detail**]

構文の説明

address {i*pv4*[*/mask*] */ipv6*[*/prefix*]}	特定の IPv4 または IPv6 アドレスの IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。ネットワークのマッピングを表示するには IPv4 サブネット マスクまたは IPv6 プレフィックスを含めます。
brief	IP アドレス セキュリティ グループ テーブル マッピングの要約を表示します。
detail	IP アドレス セキュリティ グループ テーブル マッピングを表示します。
ipv4	IPv4 アドレス セキュリティ グループ テーブル マッピングを表示します。デフォルトで、IPv4 アドレス セキュリティ グループ テーブル マップのみが表示されます。
ipv6	IPv6 アドレス セキュリティ グループ テーブル マッピングを表示します。
name	セキュリティ グループ名が一致する IP アドレス セキュリティ グループ テーブル マッピングを表示します。
sgt *sgt*	セキュリティ グループ テーブルが一致する IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	コマンドが追加されました。
9.3(1)	「CLI-HI」ソースからの IP-SGT バインディング情報が含まれるように出力が更新されました。これは、**cts role-based sgt-map** コマンドにより移入されます。
9.6(1)	ネットワーク マッピングを表示する機能が追加されました。

使用上のガイドライン

このコマンドは、制御パスの IP アドレス セキュリティ グループ テーブル マネージャ エントリを表示します。

例

次に、**show cts sgt-map** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address    SGT Source
============================================
1.1.1.1       7 CLI-HI
10.10.10.1    7 CLI-HI
10.10.10.10   3 LOCAL
10.10.100.1   7 CLI-HI
198.26.208.31 7   SXP
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of CLI-HI   bindings = 3
Total number of SXP      bindings = 1
Total number of active   bindings = 5
```

次に、いくつかのネットワーク バインドを指定した **show cts sgt-map** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address       SGT Source
============================================
10.1.1.1          7   CLI-HI
10.252.10.0/24    7   CLI-HI
10.252.10.10      3   LOCAL
10.252.100.1      7   CLI-HI
172.26.0.0/16     7   SXP
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of CLI-HI   bindings = 3
Total number of SXP      bindings = 1
Total number of active   bindings = 5
```

次に、**show cts sgt-map ipv6** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map ipv6
Active IP-SGT Bindings Information

IP Address                                SGT     Source
============================================================
3330::1                                   17      SXP
FE80::A8BB:CCFF:FE00:110                  17      SXP

IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 2
Total number of active   bindings = 2
```

次に、**show cts sgt-map ipv6 detail** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map ipv6 detail
Active IP-SGT Bindings Information

IP Address                Security Group                          Source
============================================================================
```

```
3330::1                     2345                                    SXP
1280::A8BB:CCFF:FE00:110    Security Tech Business Unit(12345)      SXP

IP-SGT Active Bindings Summary
==================================
Total number of SXP bindings    = 2
Total number of active bindings = 2
```

次に、**show cts sgt-map ipv6 brief** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map ipv6 brief
Active IP-SGT Bindings Information

IP-SGT Active Bindings Summary
==================================
Total number of SXP bindings    = 2
Total number of active bindings = 2
```

次に、**show cts sgt-map address** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map address 10.10.10.5

Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================================
10.10.10.5              1234    SXP

IP-SGT Active Bindings Summary
==========================================
Total number of SXP    bindings = 1
Total number of active   bindings = 1
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show cts sxp connections

ASA に Security eXchange Protocol（SXP）接続を表示するには、特権 EXEC モードで **show cts sxp connections** コマンドを使用します。

show cts sxp connections [**peer** *peer addr*] [**local** *local addr*] [**ipv4 | ipv6**] [**status** {**on | off | delete-hold-down | pending-on**}] [**mode** {**speaker | listener**}] [**brief**]

構文の説明

brief	（オプション）SXP 接続の要約を表示します。
delete-hold-down	（オプション）TCP 接続は ON 状態であったときに終了しました（TCP がダウンしています）。この状態になる可能性があるのは、リスナー モードで設定された ASA のみです。
ipv4	（オプション）IPv4 アドレスとの SXP 接続を表示します。
ipv6	（オプション）IPv6 アドレスとの SXP 接続を表示します。
listener	（オプション）リスナー モードで設定された ASA を表示します。
local *local addr*	（オプション）一致したローカル IP アドレスとの SXP 接続を表示します。
mode	（オプション）一致したモードとの SXP 接続を表示します。
off	（オプション）TCP 接続は開始されていません。ASA は、この状態のときのみ TCP 接続を再試行します。
on	（オプション）SXP OPEN または SXP OPEN RESP メッセージを受信しました。SXP 接続が正常に確立されました。ASA は、この状態のときのみ SXP メッセージを交換します。
peer *peer addr*	（オプション）一致したピア IP アドレスとの SXP 接続を表示します。
pending-on	（オプション）SXP OPEN メッセージがピアに送信されました。ピアからの応答を待機しています。
speaker	（オプション）スピーカー モードで設定された ASA を表示します。
status	（オプション）一致したステータスとの SXP 接続を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	コマンドが追加されました。

使用上のガイドライン

次の条件に該当する場合、SXP 状態が変わります。

- ピアが SXP の設定を解除したり、SXP をディセーブルにしたために、SXP リスナーがその SXP 接続をドロップした場合、SXP リスナーは OFF 状態に移行します。
- ピアがクラッシュしたり、インターフェイスがシャットダウンしたために、SXP リスナーがその SXP 接続をドロップした場合、SXP リスナーは DELETE_HOLD_DOWN 状態に移行します。
- 最初の 2 つの条件のいずれかが発生すると、SXP スピーカーは OFF 状態に移行します。

このコマンドは、フェールオーバー モードのアクティブなデバイスとマスター ユニット クラスタのみでサポートされます。

例

次に、**show cts sxp connections** コマンドの出力例を示します。

```
ciscoasa# show cts sxp connections
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local IP   : Not Set
Delete hold down period : 120 secs
Reconcile period   : 120 secs
Retry open period : 10 secs
Retry open timer   : Not Running
Total number of SXP connections : 3
Total number of SXP connection shown : 3
----------------------------------------------
Peer IP            : 2.2.2.1
Local IP           : 2.2.2.2
Conn status        : On
Local mode         : Listener
Ins number         : 1
TCP conn password : Default
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 3.3.3.1
Local IP           : 3.3.3.2
Conn status        : On
Local mode         : Listener
Ins number         : 2
TCP conn password : None
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:01:02:20 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 4.4.4.1
Local IP           : 4.4.4.2
Conn status        : On
Local mode         : Speaker
Ins number         : 1
TCP conn password : Set
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:03:01:20 (dd:hr:mm:sec)
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show cts sxp sgt-map

ASA に、Cisco TrustSec の Security eXchange Protocol（SXP）モジュール内の現在の IP アドレス セキュリティ グループ テーブル マッピング データベース エントリを表示するには、特権 EXEC モードで **show cts sxp sgt-map** コマンドを使用します。

show cts sxp sgt-map [**peer** *peer_addr*] [**sgt** *sgt*] [**address** *ipv4*[*/mask*] | **address** *ipv6*[*/prefix*] | **ipv4** | **ipv6**] [**name**] [**brief** | **detail**] [**status**]

構文の説明

address {i*pv4*[*/mask*] */ipv6*[*/prefix*]}	特定の IPv4 または IPv6 アドレスの IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。ネットワークのマッピングを表示するには IPv4 サブネット マスクまたは IPv6 プレフィックスを含めます。
brief	IP アドレス セキュリティ グループ テーブル マッピングの要約を表示します。
detail	セキュリティ グループ テーブル情報を表示します。セキュリティ グループの名前が使用できない場合、セキュリティ グループ テーブル値のみが角カッコなしで表示されます。
ipv4	IPv4 アドレスとの IP アドレス セキュリティ グループ テーブル マッピングを表示します。デフォルトで、IPv4 アドレスとの IP アドレス セキュリティ グループ テーブル マッピングのみが表示されます。
ipv6	IPv6 アドレスとの IP アドレス セキュリティ グループ テーブル マッピングを表示します。
name	セキュリティ グループ名が一致する IP アドレス セキュリティ グループ テーブル マッピングを表示します。
peer *peer addr*	ピア IP アドレスが一致する IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。
sgt *sgt*	セキュリティ グループ テーブルが一致する IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。
status	アクティブまたは非アクティブなマッピング済みエントリを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	コマンドが追加されました。
9.6(1)	ネットワーク マッピングを表示する機能が追加されました。

使用上のガイドライン

このコマンドは、SXP から統合されたアクティブな IP アドレス セキュリティ グループ テーブルのマッピング済みエントリを表示します。

このコマンドは、フェールオーバー コンフィギュレーションのスタンバイ状態のデバイスではサポートされません。クラスタでは、マスター ユニットでコマンドを入力します。

例

次に、**show cts sxp sgt-map** コマンドの出力例を示します。

```
ciscoasa# show cts sxp sgt-map
Total number of IP-SGT mappings : 3

SGT        : 7
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1

SGT        : 7
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1

SGT        : 7
IPv6       : FE80::A8BB:CCFF:FE00:110
Peer IP    : 2.2.2.1
Ins Num    : 1
```

次に、**show cts sxp sgt-map detail** コマンドの出力例を示します。

```
ciscoasa# show cts sxp sgt-map detail
Total number of IP-SGT mappings : 3

SGT        : STBU(7)
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active

SGT        : STBU(7)
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1
Status     : Inactive

SGT        : 6
IPv6       : 1234::A8BB:CCFF:FE00:110
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active
```

次に、**show cts sxp sgt-map brief** コマンドの出力例を示します。一部のマッピングはネットワークに繋がります。

```
ciscoasa# show cts sxp sgt-map brief
Total number of IP-SGT mappings : 3
SGT, IPv4: 7, 2.2.2.0/24
SGT, IPv4: 7, 3.3.3.3
SGT, IPv6: 7, FE80::0/64
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show curpriv

現在のユーザ特権を表示するには、**show curpriv** コマンドを使用します。

show curpriv

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	• 対応
特権 EXEC	• 対応	• 対応	—	—	• 対応
ユーザ EXEC	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに準拠するように変更されました。

使用上のガイドライン

show curpriv コマンドは、現在の特権レベルを表示します。特権レベルの数値が小さいほど、特権レベルが低いことを示しています。

例

次に、enable_15 という名前のユーザが異なる特権レベルにある場合の **show curpriv** コマンドの出力例を示します。ユーザ名は、ユーザがログインしたときに入力した名前を示しています。P_PRIV は、ユーザが **enable** コマンドを入力したことを示しています。P_CONF は、ユーザが **config terminal** コマンドを入力したことを示します。

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit

ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa(config)# exit
```

```
ciscoasa(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa(config)#
```

次に、既知の動作の例を示します。イネーブル モードからディセーブル モードに移行した場合、最初にログインしたユーザ名が enable_1 に置き換わります。

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# exit

Logoff

Type help or '?' for a list of available commands.
ciscoasa# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
show running-config privilege	コマンドの特権レベルを表示します。

show ddns update interface コマンド～ show event manager コマンド

show ddns update interface

ASA インターフェイスに割り当てられた DDNS 方式を表示するには、特権 EXEC モードで **show ddns update interface** コマンドを使用します。

show ddns update interface [*interface-name*]

構文の説明

interface-name	(任意) ネットワーク インターフェイスの名前。

デフォルト

interface-name ストリングを省略すると、各インターフェイスに割り当てられている DDNS 方式が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、内部インターフェイスに割り当てられている DDNS 方式を表示する例を示します。

```
ciscoasa# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
ciscoasa#
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（**インターフェイス コンフィギュレーション モード**）	ASA インターフェイスを DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（**グローバル コンフィギュレーション モード**）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show ddns update method	設定済みの各 DDNS 方式のタイプと間隔を表示します。DDNS 更新を実行する DHCP サーバ。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

show ddns update method

実行コンフィギュレーションの DDNS 更新方式を表示するには、特権 EXEC モードで **show ddns update method** コマンドを使用します。

show ddns update method [*method-name*]

構文の説明

method-name	（任意）設定済み DDNS 更新方式の名前。

デフォルト

method-name ストリングを省略すると、設定されているすべての DDNS 更新方式が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ddns-2 という名前の DDNS 方式を表示する例を示します。

```
ciscoasa(config)# show ddns update method ddns-2

Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
ciscoasa(config)#
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（**インターフェイス コンフィギュレーション モード**）	ASA インターフェイスをダイナミック DNS（DDNS）更新方式または DDNS 更新ホスト名に関連付けます。
ddns update method（**グローバル コンフィギュレーション モード**）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。

コマンド	説明
show ddns update interface	設定済みの各 DDNS 方式に関連付けられたインターフェイスを表示します。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

show debug

現在のデバッグ コンフィギュレーションを表示するには、**show debug** コマンドを使用します。

show debug [*command* [*keywords*]]

構文の説明

command	（オプション）現在の設定を表示する **debug** コマンドを指定します。
キーワード	（オプション）各 *command* について、*command* に続く *keywords* は、関連する **debug** コマンドによりサポートされる *keywords* と同一です。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	使用可能なコマンド値のリストに **eigrp** キーワードが追加されました。
8.4(1)	使用可能なコマンド値のリストに **route** キーワードが追加されました。
9.2(1)	使用可能なコマンド値のリストに **event manager** キーワードが追加されました。
9.5(2)	デバッグの永続的な設定が含まれるように、出力が変更されました。
9.5(2)	フィルタ条件セットに基づいたフィルタリングによってデバッグ ログを表示する機能が追加されました。

使用上のガイドライン

各 *command* について、*command* に続く *keywords* は、関連する **debug** コマンドによりサポートされる *keywords* と同一です。サポートされている構文については、関連する **debug** コマンドを参照してください。

（注） 各 *command* を使用できるかどうかは、該当する **debug** コマンドをサポートするコマンド モードによって異なります。

有効な *command* 値は次のとおりです。

- **aaa**
- **appfw**
- **arp**
- **asdm**
- コンテキスト
- **crypto**
- **ctiqbe**
- **ctm**
- **cxsc**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- **event manager**
- **fixup**
- **fover**
- **fsm**
- **FTP**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**

- **mgcp**
- **mmp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**
- **route**
- **rtsp**
- **sdi**
- **sequence**
- **sfr**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**
- **xml**

例

show debug コマンドを使用して、すべてのデバッグ コンフィギュレーション、特定の機能のデバッグ コンフィギュレーション、および機能の一部に対するデバッグ コンフィギュレーションを表示できます。

次のコマンドでは、認証、アカウンティング、およびフラッシュ メモリのデバッグをイネーブルにします。

```
ciscoasa# debug aaa authentication
debug aaa authentication enabled at level 1
ciscoasa# debug aaa accounting
```

```
debug aaa accounting enabled at level 1
ciscoasa# debug disk filesystem
debug disk filesystem enabled at level 1
ciscoasa# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
ciscoasa# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
ciscoasa# show debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa#
```

関連コマンド

コマンド	説明
debug	すべての **debug** コマンドを表示します。

show dhcpd

DHCP のバインディング情報、状態情報、および統計情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcpd** コマンドを使用します。

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

構文の説明

binding	所定のサーバ IP アドレスおよび関連するクライアント ハードウェア アドレスについてのバインディング情報とリースの長さを表示します。
IP_address	指定した IP アドレスのバインディング情報を表示します。
state	DHCP サーバの状態（現在のコンテキストでイネーブルかどうか、各インターフェイスについてイネーブルかどうかなど）を表示します。
statistics	統計情報（アドレス プール、バインディング、期限切れバインディング、不正な形式のメッセージ、送信済みメッセージ、および受信メッセージなどの数）を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

オプションの IP アドレスを **show dhcpd binding** コマンドに含めた場合は、その IP アドレスのバインディングだけが表示されます。

show dhcpd binding | state | statistics コマンドはグローバル コンフィギュレーション モードでも使用可能です。

例

次に、**show dhcpd binding** コマンドの出力例を示します。

```
ciscoasa# show dhcpd binding
IP Address Client-id       Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

次に、**show dhcpd state** コマンドの出力例を示します。

```
ciscoasa# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

次に、**show dhcpd statistics** コマンドの出力例を示します。

```
ciscoasa# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
clear dhcpd	DHCP サーバ バインディングおよび統計情報カウンタをクリアします。
dhcpd lease	クライアントに付与される DHCP 情報のリースの長さを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

show dhcprelay state

DHCP リレー エージェントの状態を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcprelay state** コマンドを使用します。

show dhcprelay state

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、現在のコンテキストおよび各インターフェイスについての DHCP リレー エージェントの状態情報を表示します。

例

次に、**show dhcprelay state** コマンドの出力例を示します。

```
ciscoasa# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

関連コマンド

コマンド	説明
show dhcpd	DHCP サーバの統計情報と状態情報を表示します。
show dhcprelay statistics	DHCP リレーの統計情報を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

show dhcprelay statistics

DHCP リレーの統計情報を表示するには、特権 EXEC モードで **show dhcprelay statistics** コマンドを使用します。

show dhcprelay statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show dhcprelay statistics コマンドの出力は、**clear dhcprelay statistics** コマンドを入力するまで増加します。

例

次に、**show dhcprelay statistics** コマンドの出力例を示します。

```
ciscoasa# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェントの統計カウンタをクリアします。
debug dhcprelay	DHCP リレー エージェントのデバッグ情報を表示します。
show dhcprelay state	DHCP リレー エージェントの状態を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

show diameter

各 Diameter 接続の状態情報を表示するには、特権 EXEC モードで **show diameter** コマンドを使用します。

show diameter

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

Diameter 接続の状態情報を表示するには、Diameter トラフィックを検査する必要があります。

例

次に、**show diameter** コマンドの出力例を示します。

```
ciscoasa# show diameter
Total active diameter sessions: 5
Session 3638
          ==========
          ref_count: 1 val = .; 1096298391; 2461;
              Protocol : diameter Context id : 0
              From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

関連コマンド

コマンド	説明
clear service-policy	サービス ポリシーの統計情報をクリアします。
inspect diameter	Diameter トラフィックを検査します。

show disk

ASA のフラッシュ メモリの内容だけを表示するには、特権 EXEC モードで **show disk** コマンドを使用します。

show disk[**0** | **1**] [**filesys** | **all**] **controller**

構文の説明

0	**1**	内部フラッシュ メモリ(0、デフォルト)または外部フラッシュ メモリ(1)を指定します。
all	フラッシュ メモリの内容とファイル システム情報を表示します。
コントローラ	フラッシュ コントローラのモデル番号を指定します。
filesys	コンパクト フラッシュ カードについての情報を表示します。

デフォルト

デフォルトでは、このコマンドは内部フラッシュ メモリを示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show disk** コマンドの出力例を示します。

```
ciscoasa# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
```

```
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

次に、**show disk filesys** コマンドの出力例を示します。

```
ciscoasa# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

次に、**show disk controller** コマンドの出力例を示します。

```
ciscoasa# show disk:1 controller
Flash Model: TOSHIBA THNCF064MBA
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。

show dns

すべてまたは指定された完全修飾ドメイン名（FQDN）ホストの現在の解決済み DNS アドレスを表示するには、特権 EXEC モードで **show dns** コマンドを使用します。

show dns [**host** *fqdn_name*]

構文の説明

fqdn_name	（オプション）選択したホストの FQDN を指定します。
ホスト	（オプション）指定したホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show dns** コマンドの出力例を示します。

```
ciscoasa# show dns
Name:   www.example1.com
  Address: 10.1.3.1                          TTL 00:03:01
  Address: 10.1.3.3                          TTL 00:00:36
  Address: 10.4.1.2                          TTL 00:01:01
Name: www.example2.com
  Address: 10.2.4.1                          TTL 00:25:13
  Address: 10.5.2.1                          TTL 00:25:01
Name: server.ddns-exampleuser.com
  Address: fe80::21e:8cff:feb5:4faa          TTL 00:00:41
  Address: 10.10.10.2                        TTL 00:25:01
```

（注） FQDN ホストがアクティブ化されていない場合は、このコマンドによる出力はありません。

次に、**show dns host** コマンドの出力例を示します。

```
ciscoasa# show dns host www.example.com
Name:   www.example.com
Address: 10.1.3.1 TTL 00:03:01
Address: 10.1.9.5 TTL 00:00:36
Address: 10.1.1.2 TTL 00:01:01
```

関連コマンド

コマンド	説明
clear dns-hosts	DNS キャッシュをクリアします。
dns domain-lookup	ASA によるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。

show dns-hosts

DNS キャッシュを表示するには、特権 EXEC モードで **show dns-hosts** コマンドを使用します。DNS キャッシュには、DNS サーバからのダイナミックに学習されたエントリおよび手動で入力された名前と IP アドレスが含まれます。

show dns-hosts

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show dns-hosts** コマンドの出力例を示します。

```
ciscoasa# show dns-hosts
Host                        Flags      Age Type   Address(es)
ns2.example.com             (temp, OK) 0    IP    10.102.255.44
ns1.example.com             (temp, OK) 0    IP    192.168.241.185
snowmass.example.com        (temp, OK) 0    IP    10.94.146.101
server.example.com          (temp, OK) 0    IP    10.94.146.80
```

関連コマンド

コマンド	説明
clear dns-hosts	DNS キャッシュをクリアします。
dns domain-lookup	ASA によるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。

表 11 に、各フィールドの説明を示します。

表 6-1　show dns-hosts の各フィールド

フィールド	説明
ホスト	ホスト名を表示します。
Flags	次の組み合わせとしてエントリのステータスを表示します。 • temp: このエントリは DNS サーバから取得されたため、一時的です。ASA は、72 時間の無活動後にこのエントリを削除します。 • perm: このエントリは **name** コマンドを使用して追加されたため、永続的です。 • OK: このエントリは有効です。 • ??: このエントリは疑わしいため、再検証が必要です。 • EX: このエントリは期限切れです。
Age	このエントリが最後に参照されてからの時間数を表示します。
タイプ	DNS レコードのタイプを表示します。この値は常に IP です。
Address(es)	IP アドレス。

関連コマンド

コマンド	説明
clear dns-hosts	DNS キャッシュをクリアします。
dns domain-lookup	ASA によるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。

show dynamic-filter data

ボットネット トラフィック フィルタ ダイナミック データベースに関する情報（ダイナミック データベースの最終ダウンロード日、データベースのバージョン情報、データベース内のエントリ数、10 個のサンプル エントリなど）を表示するには、特権 EXEC モードで **show dynamic-filter data** コマンドを使用します。

show dynamic-filter data

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

ダイナミック データベース情報を表示するには、最初に **dynamic-filter use-database** コマンドと **dynamic-filter updater-client enable** コマンドを使用して、データベースの使用とダウンロードをイネーブルにします。

例

次に、**show dynamic-filter data** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter data

Traffic filter is using downloaded database version '907'
Fetched at 18:00:16 UTC Jan 22 2009, size: 674381
Sample names from downloaded database:
  example.com, example.net, example.org,
cisco.example, cisco.invalid, bad.example.com
bad.example.net, bad.example.org, bad.cisco.example
bad.cisco.ivalid
```

```
Total entries in Dynamic Filter database:
  Dynamic data: 40909 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
  Dynamic data: 0 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。

コマンド	説明
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

show dynamic-filter dns-snoop

ボットネット トラフィック フィルタの DNS スヌーピング サマリー（または実際の IP アドレスと名前）を表示するには、特権 EXEC モードで **show dynamic-filter dns-snoop** コマンドを使用します。

show dynamic-filter dns-snoop [**detail**]

構文の説明

detail	（任意）DNS 応答からスヌーピングされた IP アドレスと名前を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

この出力には、ブラックリストに一致する名前だけでなく、すべての検査済み DNS データが含まれます。スタティック エントリの DNS データは含まれません。

DNS スヌーピング データを消去するには、**clear dynamic-filter dns-snoop** コマンドを入力します。

例

次に、**show dynamic-filter dns-snoop** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter dns-snoop

DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
```

次に、**show dynamic-filter dns-snoop detail** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter dns-snoop detail

DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
```

```
DNS reverse Cache Information:
[10.67.22.34] flags=0x22, cat=2, unit=0 b:g:w=3:0:0, cookie=0xda148218
    [www3.example.com] cat=2, ttl=3
    [www.bad.example.com] cat=2, ttl=3
    [www.example.com] cat=2, ttl=3
[10.6.68.133] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda13ed60
    [cisco.example] cat=2, ttl=73
[10.166.226.25] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda608cb8
    [cisco.invalid] cat=2, ttl=2
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。

コマンド	説明
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

show dynamic-filter reports infected-hosts

ボットネット トラフィック フィルタで分類された、感染したホストのレポートを生成するには、特権 EXEC モードで **show dynamic-filter reports infected-hosts** コマンドを使用します。

show dynamic-filter reports infected-hosts {**max-connections** | **latest-active** | **highest-threat** | **subnet** *ip_address netmask* | **all**}

構文の説明

all	バッファに格納されている感染したホストの情報をすべて表示します。この表示には、数千ものエントリが含まれることがあります。CLI ではなく、ASDM を使用して PDF を生成できます。
highest-threat	脅威レベルが最高のマルウェア サイトに接続する 20 個のホストを表示します。
latest-active	最近アクティビティを行った 20 個のホストを表示します。各ホストについて、アクセスした 5 件のマルウェア サイトに関する詳細情報が表示されます。
max-connections	接続数が最も多い感染ホストを 20 個表示します。
subnet *ip_address netmask*	指定されたサブネット内のホストを最大 20 個表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

これらのレポートには、感染ホストの詳細な履歴が含まれ、感染ホスト、閲覧したマルウェア サイト、およびマルウェア ポートを示します。

レポート データを消去するには、**clear dynamic-filter reports infected-hosts** コマンドを入力します。

例

次に、**show dynamic-filter reports infected hosts all** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter reports infected-hosts all

Total 2 infected-hosts in buffer
Host (interface)                        Latest malicious conn time, filter action  Conn logged, dropped
=============================================================================================================
192.168.1.4 (internal)                  15:39:40 UTC Sep 17 2009, dropped                    3      3
Malware-sites connected to (not ordered)
Site                       Latest conn port, time, filter action   Conn logged, dropped Threat-level Category
-------------------------------------------------------------------------------------------------------------
10.73.210.27 (bad.example.com)     80, 15:39:31 UTC Sep 17 2009, dropped      2   2     very-high Malware
10.65.2.119 (bad2.example.com)     0, 15:39:40 UTC Sep 17 2009, dropped       1   1     very-high admin-added
=============================================================================================================
192.168.1.2 (internal)                  15:39:01 UTC Sep 17 2009, dropped                    5      5
Malware-sites connected to (not ordered)
Site                       Latest conn port, time, filter action   Conn logged, dropped Threat-level Category
-------------------------------------------------------------------------------------------------------------
10.131.36.158 (bad.example.com)    0, 15:37:46 UTC Sep 17 2009, dropped      1    1    very-high admin-added
10.65.2.119 (bad2.example.com)     0, 15:37:53 UTC Sep 17 2009, dropped      1    1   very-high  admin-added
20.73.210.27 (bad3.example.com)   80, 15:39:01 UTC Sep 17 2009, dropped      3    3   very-high  Malware
=============================================================================================================

Last clearing of the infected-hosts report: Never
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。

コマンド	説明
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

show dynamic-filter reports top

ボットネット トラフィック フィルタによって分類された、上位 10 件のマルウェア サイト、ポート、および感染ホストのレポートを生成するには、特権 EXEC モードで **show dynamic-filter reports top** コマンドを使用します。

show dynamic-filter reports top [**malware-sites** | **malware-ports** | **infected-hosts**]

構文の説明

malware-ports	（任意）上位 10 件のマルウェア サイトのレポートを表示します。
malware-sites	（任意）上位 10 件のマルウェア ポートのレポートを表示します。
infected-hosts	（任意）上位 10 件の感染ホストのレポートを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.2(2)	**botnet-sites** キーワードおよび **botnet-ports** キーワードは **malware-sites** および **malware-ports** に変更されました。malware-sites レポートには、ドロップした接続数と、各サイトの脅威レベルおよびカテゴリが含まれています。最終クリア タイムスタンプが追加されました。脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

このレポートはデータのスナップショットで、統計情報の収集開始以降の上位 10 項目に一致しない場合があります。

レポート データを消去するには、**clear dynamic-filter reports top** コマンドを入力します。

例

次に、**show dynamic-filter reports top malware-sites** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter reports top malware-sites
Site                                  Connections logged dropped Threat Level Category
-------------------------------------------------------------------------------------
bad1.example.com (10.67.22.34)                    11     0          2      Botnet
bad2.example.com (209.165.200.225)                 8     8          3      Virus
bad1.cisco.example(10.131.36.158)                  6     6          3      Virus
bad2.cisco.example(209.165.201.1)                  2     2          3      Trojan
horrible.example.net(10.232.224.2)                 2     2          3      Botnet
nono.example.org(209.165.202.130)                  1     1          3      Virus

Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

次に、**show dynamic-filter reports top malware-ports** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter reports top malware-ports
Port                                          Connections logged
-----------------------------------------------------------------
tcp 1000                                                    617
tcp 2001                                                    472
tcp 23                                                       22
tcp 1001                                                     19
udp 2000                                                     17
udp 2001                                                     17
tcp 8080                                                      9
tcp 80                                                        3
tcp >8192                                                     2

Last clearing of the top ports report: at 13:41:06 UTC Jul 15 2009
```

次に、**show dynamic-filter reports top infected-hosts** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter reports top infected-hosts
Host                                          Connections logged
-----------------------------------------------------------------
10.10.10.51(inside)                                        1190
10.12.10.10(inside)                                          10
10.10.11.10(inside)                                           5

Last clearing of the top infected-hosts report: at 13:41:06 UTC Jul 15 2009
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。

コマンド	説明
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

show dynamic-filter statistics

ボットネット トラフィック フィルタを使用して、ホワイトリスト、ブラックリスト、およびグレイリストとして分類された接続の数を表示するには、特権 EXEC モードで **show dynamic-filter statistics** コマンドを使用します。

show dynamic-filter statistics [**interface** *name*] [**detail**]

構文の説明

detail	(任意)各脅威レベルで分類またはドロップされたパケットの数を表示します。
interface *name*	(任意)特定のインターフェイスの統計情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.2(2)	各脅威レベルで分類またはドロップされたパケット数を表示するための **detail** キーワードが追加されました。脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

グレイリストには、複数のドメイン名に関連付けられているが、これらすべてのドメイン名がブラックリストに記載されているわけではないアドレスが含められます。

統計情報をクリアするには、**clear dynamic-filter statistics** コマンドを入力します。

例

次に、**show dynamic-filter statistics** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter statistics
Enabled on interface outside
 Total conns classified 11, ingress 11, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
```

```
 Total blacklist classified 11, dropped 5, ingress 11, egress 0
Enabled on interface inside
 Total conns classified 1182, ingress 1182, egress 0
 Total whitelist classified 3, ingress 3, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 1179, dropped 1000, ingress 1179, egress 0
```

次に、**show dynamic-filter statistics interface outside detail** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter statistics interface outside detail
Enabled on interface outside
 Total conns classified 2108, ingress 2108, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 1, dropped 1, ingress 0, egress 0
   Threat level 5 classified 1, dropped 1, ingress 0, egress 0
   Threat level 4 classified 0, dropped 0, ingress 0, egress 0
   ...
Total blacklist classified 30, dropped 20, ingress 11, egress 2
   Threat level 5 classified 6, dropped 6, ingress 4, egress 2
   Threat level 4 classified 5, dropped 5, ingress 5, egress 0
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。

コマンド	説明
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

show dynamic-filter updater-client

ボットネット トラフィック フィルタのアップデータ サーバに関する情報（サーバの IP アドレス、ASA がサーバに接続する次のタイミング、インストールされているデータベースのバージョンなど）を表示するには、特権 EXEC モードで **show dynamic-filter updater-client** コマンドを使用します。

show dynamic-filter updater-client

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、**show dynamic-filter updater-client** コマンドの出力例を示します。

```
ciscoasa# show dynamic-filter updater-client

Traffic Filter updater client is enabled
Updater server url is https://10.15.80.240:446
Application name: trafmon, version: 1.0
Encrypted UDI:
0bb93985f42d941e50dc8f022350d1a8de96ba6c1f6d45f4bc0ead02a7d5990be32f483b
5715cd80a215cedadd4e5ffe
Next update is in 00:02:00
Database file version is '907' fetched at 22:51:41 UTC Oct 16 2006,
size: 521408
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。

コマンド	説明
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

show eigrp events

EIGRP イベント ログを表示するには、特権 EXEC モードで **show eigrp events** コマンドを使用します。

show eigrp [*as-number*] **events** [{*start end*} | **type**]

構文の説明

as-number	(任意)イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。ASA がサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
end	(任意)出力されるエントリを、インデックス番号 *start* で開始され、インデックス番号 *end* で終了するエントリに限定します。
start	(任意)ログ エントリのインデックス番号を指定する数値。開始番号を指定すると、出力は指定されたイベントで開始し、*end* 引数で指定されたイベントで終了します。有効な値は、1 ～ 4294967295 です。
type	(任意)記録されるイベントを表示します。

デフォルト

start および *end* を指定しない場合、すべてのログ エントリが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

show eigrp events の出力では最大 500 件のイベントが表示されます。イベントが最大数に到達すると、新しいイベントは出力の末尾に追加され、古いイベントは出力の先頭から削除されます。

clear eigrp events コマンドを使用すると、EIGRP イベント ログをクリアできます。

show eigrp events type コマンドは、EIGRP イベントのロギング ステータスを表示します。デフォルトでは、ネイバー変更、ネイバー警告、および DUAL FSM メッセージが記録されます。ネイバー変更イベントのロギングは、**no eigrp log-neighbor-changes** コマンドを使用してディセーブルにできます。ネイバー警告イベントのロギングは、**no eigrp log-neighbor-warnings** コマンドを使用してディセーブルにできます。DUAL FSM イベントのロギングはディセーブルにできません。

例

次に、**show eigrp events** コマンドの出力例を示します。

```
ciscoasa# show eigrp events

Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

次に、**show eigrp events** コマンドで開始番号と終了番号を定義したときの出力例を示します。

```
ciscoasa# show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

次に、EIGRP イベント ログのエントリがない場合の **show eigrp events** コマンドの出力例を示します。

```
ciscoasa# show eigrp events

Event information for AS 100:  Event log is empty.
```

次に、**show eigrp events type** コマンドの出力例を示します。

```
ciscoasa# show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

関連コマンド

コマンド	説明
clear eigrp events	EIGRP イベント ロギング バッファをクリアします。
eigrp log-neighbor-changes	ネイバー変更イベントのロギングをイネーブルにします。
eigrp log-neighbor-warnings	ネイバー警告イベントのロギングをイネーブルにします。

show eigrp interfaces

EIGRP ルーティングに参加しているインターフェイスを表示するには、特権 EXEC モードで **show eigrp interfaces** コマンドを使用します。

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

構文の説明

as-number	(任意)アクティブ インターフェイスを表示する EIGRP プロセスの自律システム番号を指定します。ASA がサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
detail	(任意)詳細情報を表示します。
if-name	(任意)**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定すると、指定されたインターフェイスに表示が制限されます。

デフォルト

インターフェイス名を指定しない場合、すべての EIGRP インターフェイスの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

show eigrp interfaces コマンドを使用して、EIGRP がアクティブなインターフェイスを判別し、それらのインターフェイスに関連する EIGRP についての情報を学習します。

インターフェイスが指定された場合、そのインターフェイスのみが表示されます。指定されない場合、EIGRP を実行しているすべてのインターフェイスが表示されます。

自律システムが指定された場合、指定された自律システムについてのルーティング プロセスのみが表示されます。指定されない場合、すべての EIGRP プロセスが表示されます。

例

次に、**show eigrp interfaces** コマンドの出力例を示します。

```
ciscoasa# show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast    Pending
Interface    Peers  Un/Reliable   SRTT   Un/Reliable   Flow Timer   Routes
mgmt           0        0/0          0      11/434          0           0
outside        1        0/0        337       0/10           0           0
inside         1        0/0         10       1/63         103           0
```

表 6-2 に、この出力で表示される重要なフィールドの説明を示します。

表 6-2　show eigrp interfaces のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Peers	直接接続されているピアの数。
Xmit Queue Un/Reliable	信頼性の低い送信キューおよび信頼性の高い送信キューに残っているパケットの数。
Mean SRTT	平均のスムーズ ラウンドトリップ時間間隔（秒）。
Pacing Time Un/Reliable	EIGRP パケット（信頼性の低いパケットおよび信頼性の高いパケット）をインターフェイスに送信するタイミングを決定するために使用されるペーシング時間（秒）。
Multicast Flow Timer	ASA がマルチキャスト EIGRP パケットを送信する最大秒数。
Pending Routes	送信キュー内で送信を待機しているパケット内のルートの数。

関連コマンド

コマンド	説明
network	EIGRP ルーティング プロセスに参加するネットワークおよびインターフェイスを定義します。

show eigrp neighbors

EIGRP ネイバー テーブルを表示するには、特権 EXEC モードで **show eigrp neighbors** コマンドを使用します。

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

構文の説明

as-number	（任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。ASA がサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
detail	（任意）詳細なネイバー情報を表示します。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定する場合、そのインターフェイスを介して学習されたすべてのネイバー テーブル エントリが表示されます。
静的	（任意）**neighbor** コマンドを使用してスタティックに定義された EIGRP ネイバーを表示します。

デフォルト

インターフェイス名を指定しない場合、すべてのインターフェイスを介して学習されたネイバーが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

clear eigrp neighbors コマンドを使用して、ダイナミックに学習されたネイバーを EIGRP ネイバー テーブルからクリアできます。

static キーワードを使用しない限り、スタティック ネイバーは出力に含まれません。

例

次に、**show eigrp neighbors** コマンドの出力例を示します。

```
ciscoasa# show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100
Address                 Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                      (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1     13       0:00:41  0      11   4     20
172.16.80.28            Ethernet0     14       0:02:01  0      10   12    24
172.16.80.31            Ethernet0     12       0:02:02  0      4    5     20
```

表 6-3 に、この出力で表示される重要なフィールドの説明を示します。

表 6-3　show eigrp neighbors フィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Address	EIGRP ネイバーの IP アドレス。
インターフェイス	ASA がネイバーから hello パケットを受信するインターフェイス。
Holdtime	ASA がダウンと宣言されるまでにネイバーからの応答を待機する時間の長さ（秒単位）。このホールド タイムは、hello パケットでネイバーから受信し、別の hello パケットをネイバーから受信するまで減少し始めます。 ネイバーがデフォルトのホールド タイムを使用している場合は、この数値は 15 未満です。ピアがデフォルト以外のホールド タイムを設定している場合は、デフォルト以外のホールド タイムが表示されます。 この値が 0 に達すると、ASA は、ネイバーを到達不能と見なします。
Uptime	ASA がこのネイバーからの応答を最初に受信してからの経過時間（時:分:秒）。
Q Count	ASA が送信を待機している EIGRP パケット（アップデート、クエリー、応答）の数。
Seq Num	ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。
SRTT	スムーズ ラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信し、ASA がそのパケットの確認応答を受信するために必要なミリ秒数です。
RTO	Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、ASA が再送信キューからネイバーにパケットを再送信するまでに待機する時間です。

次に、**show eigrp neighbors static** コマンドの出力例を示します。

```
ciscoasa# show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                Interface
192.168.1.5                   management
```

表 6-4 に、この出力で表示される重要なフィールドの説明を示します。

表 6-4　show ip eigrp neighbors static のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Static Address	EIGRP ネイバーの IP アドレス。
インターフェイス	ASA がネイバーから hello パケットを受信するインターフェイス。

次に、**show eigrp neighbors detail** コマンドの出力例を示します。

```
ciscoasa# show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

表 6-5 に、この出力で表示される重要なフィールドの説明を示します。

表 6-5　show ip eigrp neighbors details のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
H	このカラムは、指定されたネイバーとの間で確立されたピアリング セッションの順番を示します。順番は、0 から始まる連続した番号で指定されます。
Address	EIGRP ネイバーの IP アドレス。
インターフェイス	ASA がネイバーから hello パケットを受信するインターフェイス。
Holdtime	ASA がダウンと宣言されるまでにネイバーからの応答を待機する時間の長さ（秒単位）。このホールド タイムは、hello パケットでネイバーから受信し、別の hello パケットをネイバーから受信するまで減少し始めます。 ネイバーがデフォルトのホールド タイムを使用している場合は、この数値は 15 未満です。ピアがデフォルト以外のホールド タイムを設定している場合は、デフォルト以外のホールド タイムが表示されます。 この値が 0 に達すると、ASA は、ネイバーを到達不能と見なします。
Uptime	ASA がこのネイバーからの応答を最初に受信してからの経過時間（時:分:秒）。
SRTT	スムーズ ラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信し、ASA がそのパケットの確認応答を受信するために必要なミリ秒数です。

表 6-5　show ip eigrp neighbors details のフィールドの説明(続き)

フィールド	説明
RTO	Retransmission Timeout(再送信のタイムアウト)(ミリ秒)。これは、ASAが再送信キューからネイバーにパケットを再送信するまでに待機する時間です。
Q Count	ASA が送信を待機している EIGRP パケット(アップデート、クエリー、応答)の数。
Seq Num	ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。
Version	指定されたピアが実行中のソフトウェア バージョン。
Retrans	パケットを再送した回数。
Retries	パケットの再送を試行した回数。
Restart time	指定されたネイバーが再起動してからの経過時間(時:分:秒)。

関連コマンド

コマンド	説明
clear eigrp neighbors	EIGRP ネイバー テーブルをクリアします。
debug eigrp neighbors	EIGRP ネイバー デバッグ メッセージを表示します。
debug ip eigrp	EIGRP パケット デバッグ メッセージを表示します。

show eigrp topology

EIGRP トポロジ テーブルを表示するには、特権 EXEC モードで **show eigrp topology** コマンドを使用します。

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

構文の説明

active	(任意)EIGRP トポロジ テーブル内のアクティブ エントリのみ表示します。
all-links	(任意)EIGRP トポロジ テーブル内のすべてのルート(フィジブル サクセサでない場合も)を表示します。
as-number	(任意)EIGRP プロセスの自律システム番号を指定します。ASA がサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
ip-addr	(オプション)表示するトポロジ テーブルからの IP アドレスを定義します。マスクと一緒に指定した場合、エントリの詳細な説明が提供されます。
mask	(オプション)*ip-addr* 引数に適用するネットワーク マスクを定義します。
pending	(任意)ネイバーからの更新を待機しているか、ネイバーへの応答を待機している、EIGRP トポロジ テーブル内のすべてのエントリを表示します。
summary	(任意)EIGRP トポロジ テーブルの要約を表示します。
zero-successors	(任意)EIGRP トポロジ テーブル内の使用可能なルートを表示します。

デフォルト

フィジブル サクセサであるルートのみが表示されます。**all-links** キーワードを使用すると、フィジブル サクセサでないものも含めたすべてのルートが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

clear eigrp topology コマンドを使用して、ダイナミック エントリをトポロジ テーブルから削除できます。

例

次に、**show eigrp topology** コマンドの出力例を示します。

コマンド履歴

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

表 6-6 に、この出力で表示される重要なフィールドの説明を示します。

表 6-6　show eigrp topology のフィールド情報

フィールド	説明
Codes	このトポロジ テーブル エントリの状態。Passive および Active は、この宛先に関する EIGRP 状態を示し、Update、Query、および Reply は、送信中のパケットのタイプを示します。
P - Passive	ルートは良好だと認識され、この宛先についての EIGRP 計算は実行されません。
A - Active	この宛先についての EIGRP 計算が実行されます。
U - Update	この宛先に更新パケットが送信されたことを示します。
Q - Query	この宛先にクエリー パケットが送信されたことを示します。
R - Reply	この宛先に応答パケットが送信されたことを示します。
r - Reply status	ソフトウェアがクエリーを送信し、応答を待機しているときに設定されるフラグ。
address mask	宛先の IP アドレスとマスク。
successors	サクセサの数。この数値は、IP ルーティング テーブル内のネクストホップの数に対応します。「successors」が大文字で表示される場合、ルートまたはネクスト ホップは遷移状態です。
FD	フィジブル ディスタンス。フィジブル ディスタンスは、宛先に到達するための最適なメトリックか、ルートがアクティブだったときに認識された最適なメトリックです。この値はフィジビリティ条件チェックに使用されます。レポートされたルータのディスタンス（スラッシュの後のメトリック）がフィジブル ディスタンスより小さい場合、フィジビリティ条件が満たされて、そのパスはフィジブル サクセサになります。ソフトウェアによってパスがフィジブル サクセサだと判断されると、その宛先にクエリーを送信する必要はありません。

表 6-6　show eigrp topology のフィールド情報(続き)

フィールド	説明
via	この宛先についてソフトウェアに通知したピアの IP アドレス。これらのエントリの最初の *n* 個(*n* はサクセサの数)は、現在のサクセサです。リスト内の残りのエントリはフィジブル サクセサです。
(*cost*/*adv_cost*)	最初の数値は宛先へのコストを表す EIGRP メトリックです。2 番めの数値はこのピアがアドバタイズした EIGRP メトリックです。
interface	情報の学習元のインターフェイス。

次に、IP アドレスとともに使用した **show eigrp topology** の出力例を示します。出力は内部ルートについてのものです。

```
ciscoasa# show eigrp topology 10.2.1.0 255.255.255.0

EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

次に、IP アドレスとともに使用した **show eigrp topology** の出力例を示します。出力は外部ルートについてのものです。

```
ciscoasa# show eigrp topology 10.4.80.0 255.255.255.0


EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
            External data:
                Originating router is 10.89.245.1
                AS number of route is 0
                External protocol is Connected, external metric is 0
                Administrator tag is 0 (0x00000000)
```

関連コマンド

コマンド	説明
clear eigrp topology	ダイナミックに検出されたエントリを EIGRP トポロジ テーブルからクリアします。

show eigrp traffic

送受信された EIGRP パケットの数を表示するには、特権 EXEC モードで **show eigrp traffic** コマンドを使用します。

show eigrp [*as-number*] **traffic**

構文の説明

as-number	(任意)イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。ASA がサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

clear eigrp traffic コマンドを使用すると、EIGRP トラフィックの統計情報をクリアできます。

例

次に、**show eigrp traffic** コマンドの出力例を示します。

```
ciscoasa# show eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

表 6-7 に、この出力で表示される重要なフィールドの説明を示します。

表 6-7　show eigrp traffic フィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Hellos sent/received	送受信された hello パケットの数
Updates sent/received	送受信されたアップデート パケットの数
Queries sent/received	送受信されたクエリー パケットの数
Replies sent/received	送受信された応答パケットの数
Acks sent/received	送受信された確認応答（ACK）パケットの数
Input queue high water mark/drops	最大受信しきい値に接近している受信パケット数および廃棄パケットの数
SIA-Queries sent/received	送受信された Stuck-in-active クエリー。
SIA-Replies sent/received	送受信された Stuck-in-active 応答。

関連コマンド

コマンド	説明
debug eigrp packets	送受信された EIGRP パケットのデバッグ情報を表示します。
debug eigrp transmit	送信された EIGRP メッセージのデバッグ情報を表示します。

show environment

システム コンポーネントのシステム環境情報を表示するには、特権 EXEC モードで **show environment** コマンドを使用します。

show environment [**alarm-contact** | **driver** | **fans** | **power-consumption** | **power-supply** | **temperature**] [**chassis** | **cpu** | **voltage**]

構文の説明

alarm-contact	（オプション）ISA 3000 デバイス上の入力アラーム コンタクトの動作ステータスを表示します。
chassis	（任意）温度表示をシャーシに限定します。
cpu	（任意）温度表示をプロセッサに限定します。
driver	（オプション）環境モニタリング（IPMI）ドライバ ステータスを表示します。ドライバ ステータスは次のいずれかになります。 • RUNNING：ドライバは動作中です。 • STOPPED：エラーが原因でドライバが停止しています。
fans	（任意）冷却ファンの動作ステータスを表示します。ステータスは次のいずれかになります。 • OK：ファンは正常に動作中です。 • Failed：ファンが故障しているため交換が必要です。
power-consumption	（オプション）PoE インターフェイスの電力消費量を表示します。
power-supply	（任意）電源の動作ステータスを表示します。各電源モジュールのステータスは次のいずれかになります。 • OK：電源は正常に動作中です。 • Failed：電源が故障しているため交換が必要です。 • Not Present：指定された電源が設置されていません。 電源モジュールの冗長性ステータスも表示されます。冗長性ステータスは次のいずれかになります。 • OK：ユニットはリソースが完全な状態で正常に動作中です。 • Lost：ユニットに冗長性はありませんが、最低限のリソースで正常に動作中です。これ以上の障害が発生した場合は、システムはシャットダウンされます。 • N/A：ユニットは電源の冗長性に対応するように設定されていません。
temperature	（任意）プロセッサとシャーシの温度およびステータスを表示します。温度は摂氏で示されます。ステータスは次のいずれかになります。 • OK：温度は通常の動作範囲内にあります。 • Critical：温度は通常の動作範囲外です。
電圧	（任意）CPU 電圧チャネル 1 ～ 24 の値を表示します。動作ステータスは除きます。

デフォルト

キーワードが指定されていない場合は、ドライバを除くすべての動作情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。
8.4(2)	ASA 5585-X SSP の出力が追加されました。さらに、デュアル SSP インストールのサポートが追加されました。
8.4.4(1)	ASA 5515-X、ASA 5525-X、5545-X、および ASA 5555-X で表示される電源温度が、出力で変更されました。
8.6(1)	ASA 5545-X および ASA 5555-X の CPU 電圧レギュレータ温度イベントの出力が追加されました。電源入力ステータスの出力が追加されました。電圧センサーの出力が追加されました。
9.7(1)	ISA 3000 用に **alarm contact** キーワードが追加されました。
9.13(1)	Firepower 1010 PoE インターフェイスに **power-consumption** キーワードが追加されました。

使用上のガイドライン

デバイスの物理コンポーネントの動作環境情報を表示できます。この情報には、ファンおよび電源の動作ステータスと、CPU およびシャーシの温度およびステータスが含まれます。ISA 3000 デバイスには、入力アラーム コンタクトに関する情報が含まれています。

（注） デュアル SSP インストールの場合、冷却ファンおよび電源の出力は、シャーシ マスターのセンサーによってのみ示されます。

例

次に、**show environment** コマンドの一般的な出力例を示します。

```
ciscoasa# show environment

Cooling Fans:
-----------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan) Power Supplies:
-----------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   --------------------------------
```

```
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
-----------------------------------
   Processors:
   --------------------------------
   Processor 1: 44.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 45.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   --------------------------------
   Ambient 1: 28.0 C - OK  (Chassis Front Temperature)
   Ambient 2: 40.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 28.0 C - OK  (CPU1 Front Temperature)
   Ambient 4: 36.50 C - OK  (CPU1 Back Temperature)
   Ambient 5: 34.50 C - OK  (CPU2 Front Temperature)
   Ambient 6: 43.25 C - OK  (CPU2 Back Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
```

次に、**show environment driver** コマンドの出力例を示します。

```
ciscoasa# show environment driver

Cooling Fans:
-----------------------------------

   Chassis Fans:
   --------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5632 RPM - OK
   Cooling Fan 3: 5888 RPM - OK

   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK

Power Supplies:
-----------------------------------

   Left Slot (PS0): Not Present
   Right Slot (PS1): Present

   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK

   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK

Temperature:
-----------------------------------

   Processors:
   --------------------------------
   Processor 1: 70.0 C - OK

   Chassis:
   --------------------------------
```

```
   Ambient 1: 36.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 31.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 39.0 C - OK  (Chassis Back Left Temperature)

   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK

Voltage:
---------------------------------
   Channel 1:  1.168 V -  (CPU Core 0.46V-1.4V)
   Channel 2: 11.954 V -  (12V)
   Channel 3:  4.998 V -  (5V)
   Channel 4:  3.296 V -  (3.3V)
   Channel 5:  1.496 V -  (DDR3 1.5V)
   Channel 6:  1.048 V -  (PCH 1.5V)
```

次に、ASA 5555-X の場合の **show environment** コマンドの出力例を示します。

```
ciscoasa# show environment

Cooling Fans:
---------------------------------

   Chassis Fans:
   --------------------------------

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 9728 RPM - OK
   Right Slot (PS1): 0 RPM - OK

Power Supplies:
 ---------------------------------

    Left Slot (PS0): Present
    Right Slot (PS1): Present

    Power Input:
    --------------------------------
    Left Slot (PS0): OK
    Right Slot (PS1): Failure Detected

    Temperature:
    --------------------------------
    Left Slot (PS0): 29 C - OK
    Right Slot (PS1): N/A

   Processors:
   --------------------------------
   Processor 1: 81.0 C - OK

   Chassis:
   --------------------------------
   Ambient 1: 39.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 32.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 47.0 C - OK  (Chassis Back Left Temperature)

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 33 C - OK
   Right Slot (PS1): -128 C - OK
```

次に、デュアル SSP インストールの ASA 5585-X シャーシ マスターの場合の **show environment** コマンドの出力例を示します。

```
ciscoasa(config)# show environment

Cooling Fans:
-----------------------------------

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)

Power Supplies:
-----------------------------------
   Power Supply Unit Redundancy: N/A

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)

Temperature:
-----------------------------------

   Processors:
   --------------------------------
   Processor 1: 48.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 47.0 C - OK  (CPU2 Core Temperature)

   Chassis:
   --------------------------------
   Ambient 1: 25.5 C - OK  (Chassis Front Temperature)
   Ambient 2: 37.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 31.50 C - OK  (CPU1 Back Temperature)
   Ambient 4: 27.75 C - OK  (CPU1 Front Temperature)
   Ambient 5: 38.25 C - OK  (CPU2 Back Temperature)
   Ambient 6: 34.0 C - OK  (CPU2 Front Temperature)

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)

Voltage:
-----------------------------------
   Channel 1:  3.310 V -  (3.3V (U142 VX1))
   Channel 2:  1.492 V -  (1.5V (U142 VX2))
   Channel 3:  1.053 V -  (1.05V (U142 VX3))
   Channel 4:  3.328 V -  (3.3V_STDBY (U142 VP1))
   Channel 5: 11.675 V -  (12V (U142 VP2))
   Channel 6:  4.921 V -  (5.0V (U142 VP3))
   Channel 7:  6.713 V -  (7.0V (U142 VP4))
   Channel 8:  9.763 V -  (IBV (U142 VH))
   Channel 9:  1.048 V -  (1.05VB (U209 VX2))
   Channel 10:  1.209 V -  (1.2V (U209 VX3))
   Channel 11:  1.109 V -  (1.1V (U209 VX4))
   Channel 12:  0.999 V -  (1.0V (U209 VX5))
   Channel 13:  3.324 V -  (3.3V STDBY (U209 VP1))
```

```
   Channel 14:  2.504 V -  (2.5V (U209 VP2))
   Channel 15:  1.799 V -  (1.8V (U209 VP3))
   Channel 16:  1.899 V -  (1.9V (U209 VP4))
   Channel 17:  9.763 V -  (IBV (U209 VH))
   Channel 18:  2.048 V -  (VTT CPU0 (U83 VX2))
   Channel 19:  2.048 V -  (VTT CPU1 (U83 VX3))
   Channel 20:  2.048 V -  (VCC CPU0 (U83 VX4))
   Channel 21:  2.048 V -  (VCC CPU1 (U83 VX5))
   Channel 22:  1.516 V -  (1.5VA (U83 VP1))
   Channel 23:  1.515 V -  (1.5VB (U83 VP2))
   Channel 24:  8.937 V -  (IBV (U83 VH))
```

CPU 電圧レギュレータ温度イベントにより ASA がシャットダウンされた場合は、次の警告メッセージが表示されます。

```
WARNING: ASA was previously shut down due to a CPU Voltage Regulator running beyond the
max thermal operating temperature. The chassis and CPU need to be inspected immediately
for ventilation issues.
```

詳細については、syslog メッセージ ガイド の syslog メッセージ 735024 を参照してください。

次に、**sshow environment alarm-contact** コマンドの出力例を示します。

```
ciscoasa> show environment alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: external alarm contact 1
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 2
   Status:      not asserted
   Description: external alarm contact 2
   Severity:    minor
   Trigger:     closed
```

関連コマンド

コマンド	説明
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。
show facility-alarm relay	トリガーされたアラームのステータス情報を表示します。
show version	ハードウェアおよびソフトウェアのバージョンを表示します。

show event manager

設定された各イベント マネージャ アプレットに関する情報を表示するには、特権 EXEC モードで **show event manager** コマンドを使用します。

show event manager

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次に、**show event manager** コマンドの出力例を示します。

```
ciscoasa# show event manager

event manager applet 21, hits 1, last 2014/01/19 06:47:46
  last file disk0:/eem-21-20140119-064746.log
  event countdown 21 secs, left 0 secs, hits 1, last 2014/01/19 06:47:47
  action 1 cli command "sh ver", hits 1, last 2014/01/19 06:47:46
```

関連コマンド

コマンド	説明
show running-config event manager	イベント マネージャの実行コンフィギュレーションを表示します。

show facility-alarm コマンド～ show ipsec stats コマンド

show facility-alarm

ISA 3000 のトリガーされたアラームを表示するには、ユーザ EXEC モードで **show facility-alarm** コマンドを使用します。

show facility-alarm {**relay** | **status** [**info** | **major** | **minor**]}

構文の説明

relay	アラーム出力リレーを通電状態にしたアラームを表示します。
status [**info** | **major** | **minor**]	トリガーされたすべてのアラームを表示します。リストを制限するには、次のキーワードを追加します。 • **major**):すべてのメジャー重大度のアラームが表示されます。 • **minor**:すべてのマイナー重大度のアラームが表示されます。 • **info**):すべてのアラームが表示されます。このキーワードを使用すると、キーワードを使用しない場合と同じ出力になります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

アラーム出力リレーを通電したアラームだけを表示するには、**relay** キーワードを使用します。出力アラームリレーは、トリガーされたアラームを有効にするよう設定したかどうかに基づいて通電されます。アラーム出力リレーを通電すると、接続しているデバイス(点滅光やブザーなど)がアクティブになります。

アラーム アクションが外部アラーム出力リレーをトリガーしたかどうかに関わらず、トリガーされたすべてのアラームを表示するには、**status** キーワードを使用します。

次の表は出力の列について示しています。

カラム	説明
Source	アラームがトリガーされたデバイス。通常は、デバイスで設定されているホスト名です。
Severity	[Major] または [minor] です。
説明	トリガーされたアラームのタイプ。たとえば、温度、アラームの外部連絡先、冗長電源など。
Relay	外部アラーム出力リレーが通電または非通電のどちらであったか。外部出力アラームは、アラーム設定に基づいてトリガーされます。
時刻	トリガーされたアラームのタイムスタンプ。

例

次に、**show facility-alarm relay** コマンドの出力例を示します。

```
ciscoasa> show facility-alarm relay
Source    Severity   Description                          Relay      Time
ciscoasa  minor      external alarm contact 1 triggered  Energized  06:56:50 UTC Mon Sep
22 2014
```

次に、**show facility-alarm status** コマンドの出力例を示します。

```
ciscoasa> show facility-alarm status info
Source    Severity  Description                        Relay         Time
ciscoasa minor external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep 22
2014
ciscoasa minor Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep 22
2014
ciscoasa major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014
ciscoasa major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014

ciscoasa> show facility-alarm status major
Source    Severity  Description                        Relay         Time
ciscoasa  major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014
ciscoasa  major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014


ciscoasa> show facility-alarm status minor
Source    Severity  Description                          Relay         Time
```

```
ciscoasa  minor     external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep
22 2014
ciscoasa  minor     Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep
22 2014
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	入力アラーム コンタクトのステータスを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

show failover

ユニットのフェールオーバー ステータスに関する情報を表示するには、特権 EXEC モードで **show failover** コマンドを使用します。

show failover [**group** *num* | **history [details]** | **interface** | **state** | **statistics**]

構文の説明

group	指定されたフェールオーバー グループの実行状態を表示します。
history [details]	フェールオーバー履歴を表示します。フェールオーバー履歴には、アクティブ ユニットの過去のフェールオーバーでの状態変化や、状態変化の理由が表示されます。 フェールオーバー履歴には、失敗の理由と個別の詳細が含まれています。これは、トラブルシューティングに役立ちます。 ピア ユニットからのフェールオーバー履歴を表示するには details キーワードを追加します。これには、フェールオーバーでのピア ユニットの状態変化や、その状態変化の理由が含まれます。 履歴情報はデバイスをリブートするとクリアされます。
interface	フェールオーバーおよびステートフル リンク情報を表示します。
num	フェールオーバー グループの番号。
state	両方のフェールオーバー ユニットのフェールオーバー状態を表示します。表示される情報は、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。障害の理由が解消されても、障害の理由は出力に残ります。
statistics	フェールオーバー コマンド インターフェイスの送信および受信パケット数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。出力の情報が追加されました。
8.2(2)	このコマンドが変更されました。出力には、ファイアウォール インターフェイスおよびフェールオーバー インターフェイスの IPv6 アドレスが含まれます。ステートフル フェールオーバーの統計情報出力には、IPv6 ネイバー探索テーブル（IPv6 ND tbl）の更新についての情報が含まれます。
9.9.2	このコマンドが変更されました。フェールオーバー履歴の出力には、エラー理由の拡張が含まれています。 history details キーワードが追加されました。これによりピア ユニットのフェールオーバー履歴が表示されます。

使用上のガイドライン

show failover コマンドは、ダイナミック フェールオーバー情報、インターフェイス ステータス、およびステートフル フェールオーバーの統計情報を表示します。

IPv4 と IPv6 の両方のアドレスがインターフェイスで設定されている場合は、両方のアドレスが出力に表示されます。インターフェイスには複数の IPv6 アドレスを設定できるため、リンクローカル アドレスのみが表示されます。インターフェイスに IPv4 アドレスが設定されていない場合、出力の IPv4 アドレスは 0.0.0.0 として表示されます。インターフェイスに IPv6 アドレスが設定されていない場合、アドレスは単純に出力から省かれます。

Stateful Failover Logical Update Statistics 出力は、ステートフル フェールオーバーがイネーブルの場合のみ表示されます。「xerr」および「rerr」の値はフェールオーバーのエラーではなく、パケット送受信エラーの数を示します。

（注） ステートフル フェールオーバーは、ASA 5505 では使用できません。したがって、ステートフル フェールオーバーの統計情報出力も使用できません。

show failover コマンド出力で、ステートフル フェールオーバーの各フィールドには次の値があります。

- Stateful Obj の値は次のとおりです。
  - xmit：送信されたパケットの数を示します。
  - xerr：送信エラーの数を示します。
  - rcv：受信したパケットの数を示します。
  - rerr：受信エラーの数を示します。
- 各行は、次に示す特定のオブジェクト スタティック カウントを表します。
  - General：すべてのステートフル オブジェクトの合計を示します。
  - sys cmd：**login** または **stay alive** などの論理的なシステム更新コマンドを示します。
  - up time：ASA のアップ タイムの値（アクティブな ASA がスタンバイの ASA に渡す）を示します。
  - RPC services：リモート プロシージャ コール接続情報。
  - TCP conn：ダイナミック TCP 接続情報。
  - UDP conn：ダイナミック UDP 接続情報。
  - ARP tbl：ダイナミック ARP テーブル情報。

- Xlate_Timeout：接続変換タイムアウト情報を示します。
- IPv6 ND tbl：IPv6 ネイバー探索テーブル情報。
- VPN IKE upd：IKE 接続情報。
- VPN IPSEC upd：IPSec 接続情報。
- VPN CTCP upd：cTCP トンネル接続情報。
- VPN SDI upd：SDI AAA 接続情報。
- VPN DHCP upd：トンネル型 DHCP 接続情報。
- SIP Session：SIP シグナリング セッション情報。
- Route Session：ルート同期アップデートの LU 統計情報

フェールオーバー IP アドレスを入力しない場合、**show failover** コマンドでは IP アドレス 0.0.0.0 が表示され、インターフェイスのモニタリングは「waiting」状態のままになります。フェールオーバーを機能させるにはフェールオーバー IP アドレスを設定する必要があります。

表 7-1 に、フェールオーバーのインターフェイス状態の説明を示します。

表 7-1　フェールオーバー インターフェイス状態

状態	説明
標準	インターフェイスは稼働中で、ピア ユニットの対応するインターフェイスから hello パケットを受信中です。
Normal (Waiting)	インターフェイスは稼働中ですが、ピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスのスタンバイ IP アドレスが設定されていること、および 2 つのインターフェイス間の接続が存在することを確認してください。
Normal (Not-Monitored)	インターフェイスは動作中ですが、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
No Link	物理リンクがダウンしています。
No Link (Waiting)	物理リンクがダウンし、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。リンクが復元した後、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。
No Link (Not-Monitored)	物理リンクがダウンしていますが、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
Link Down	物理リンクは動作中ですが、インターフェイスは管理上ダウンしています。
Link Down (Waiting)	物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスを動作状態にした後（インターフェイス コンフィギュレーション モードで **no shutdown** コマンドを使用）、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。

表 7-1　フェールオーバー インターフェイス状態(続き)

状態	説明
Link Down (Not-Monitored)	物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
Testing	ピア ユニットの対応するインターフェイスから hello パケットが届かないため、インターフェイスはテスト モードです。
不合格	インターフェイスのテストに失敗し、インターフェイスは障害が発生したとしてマークされます。インターフェイスの障害によってフェールオーバー基準が満たされた場合、インターフェイスの障害によって、セカンダリ ユニットまたはフェールオーバー グループへのフェールオーバーが発生します。

マルチ コンテキスト モードでは、**show failover** コマンドのみがセキュリティ コンテキストで使用できます。オプションのキーワードは入力できません。

例

次に、Active/Standby フェールオーバーでの **show failover** コマンドの出力例を示します。ASA では、フェールオーバー リンク(folink)と inside インターフェイスに IPv6 アドレスを使用しています。

```
ciscoasa# show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1049 maximum
MAC Address Move Notification Interval not set
Version: Ours 98.1(1)86, Mate 98.1(1)86
Serial Number: Ours JAF1610APKQ, Mate JAF1610ALGM
Last Failover at: 12:52:34 UTC Apr 26 2017
        This host: Primary - Active
                Active time: 87 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.1): Normal (Monitored)
                  Interface outside (192.168.77.1): No Link (Waiting)
                  Interface dmz (192.168.67.1): No Link (Waiting)
                slot 1: empty
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.2): Normal (Waiting)
                  Interface outside (192.168.77.2): No Link (Waiting)
                  Interface dmz (192.168.67.2): No Link (Waiting)
                slot 1: empty
                slot 1: empty
```

```
Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/4 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         22         0          6          0
        sys cmd         6          0          6          0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         14         0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        VPN IKEv1 SA    0          0          0          0
        VPN IKEv1 P2    0          0          0          0
        VPN IKEv2 SA    0          0          0          0
        VPN IKEv2 P2    0          0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
        SIP Session     0          0          0          0
        SIP Tx  0          0          0          0
        SIP Pinhole     0          0          0          0
        Route Session   0          0          0          0
        Router ID       1          0          0          0
        User-Identity   1          0          0          0
        CTS SGTNAME     0          0          0          0
        CTS PAC         0          0          0          0
        TrustSec-SXP    0          0          0          0
        IPv6 Route      0          0          0          0
        STS Table       0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       5       6
        Xmit Q:         0       27      86
```

次に、Active/Active フェールオーバーでの **show failover** コマンドの出力例を示します。この例では、管理コンテキストでのみ IPv6 アドレスをインターフェイスに割り当てています。

```
ciscoasa# show failover

Failover On
Failover unit Primary
Failover LAN Interface: folink GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.5): Normal
                admin Interface folink (10.132.9.5/fe80::2a0:c9ff:fe03:101): Normal
                admin Interface inside (10.130.8.5/fe80::2a0:c9ff:fe01:101): Normal
                admin Interface fourth (10.130.9.5/fe80::3eff:fe11:6670): Normal
                ctx1 Interface outside (10.1.1.1): Normal
```

```
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                slot 0: ASA-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.6): Normal
                admin Interface folink (10.132.9.6/fe80::2a0:c9ff:fe03:102): Normal
                admin Interface inside (10.130.8.6/fe80::2a0:c9ff:fe01:102): Normal
                admin Interface fourth (10.130.9.6/fe80::3eff:fe11:6671): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     22         0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
        SIP Session     0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

次に、ASA 5505 シリーズのでの **show failover** コマンドの出力例を示します。

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006

        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty
```

```
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

次に、アクティブ-アクティブ セットアップでの **show failover state** コマンドの出力例を示します。

```
ciscoasa(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

次に、アクティブ-スタンバイ セットアップでの **show failover state** コマンドの出力例を示します。

```
ciscoasa(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             12:53:10 UTC Apr 26 2017

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

表 7-2 に、**show failover state** コマンドの出力の説明を示します。

表 7-2　show failover state の出力の説明

フィールド	説明
Configuration State	コンフィギュレーションの同期化の状態を表示します。 スタンバイ ユニットで可能なコンフィギュレーション状態は、次のとおりです。 • **Config Syncing - STANDBY**：コンフィギュレーションの同期化が実行されているときに設定されます。 • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**：スタンバイ ユニットが、アクティブ ユニットとのコンフィギュレーションの同期化を完了したときに設定されます。 アクティブ ユニットで可能なコンフィギュレーション状態は、次のとおりです。 • **Config Syncing**：スタンバイ ユニットに対してコンフィギュレーションの同期化を実行しているときにアクティブ ユニット上で設定されます。 • **Interface Config Syncing** • **Sync Done**：アクティブ ユニットが、スタンバイ ユニットに対してコンフィギュレーションの同期化を正常に完了したときに設定されます。 • **Ready for Config Sync**：スタンバイ ユニットがコンフィギュレーションの同期化を受信する準備が完了したという信号を送るときにアクティブ ユニット上で設定されます。
Communication State	MAC アドレスの同期化のステータスを表示します。 • **Mac set**：MAC アドレスがピア ユニットからこのユニットに同期化されました。 • **Updated Mac**：MAC アドレスが更新され、他のユニットに対して同期化する必要がある場合に使用されます。また、ユニットが遷移期間中に、ピア ユニットから同期化されたローカル MAC アドレスを更新する場合にも使用されます。
Date/Time	障害の日付およびタイムスタンプを表示します。
Last Failure Reason	最後にレポートされた障害の理由を表示します。この情報は、障害の条件が解消されてもクリアされません。この情報は、フェールオーバーが発生した場合にのみ変更されます。 可能な障害の理由は次のとおりです。 • **Interface Failure**：障害が発生したインターフェイスの数がフェールオーバー基準を満たし、フェールオーバーが発生しました。 • **Comm Failure**：フェールオーバー リンクに障害が発生したか、ピアがダウンしています。 • **Backplane Failure**

表 7-2　show failover state の出力の説明（続き）

フィールド	説明
状態	ユニットの Primary/Secondary および Active/Standby ステータスを表示します。
This host/Other host	This host は、コマンドが実行されたデバイスについての情報を示します。Other host は、フェールオーバーのペアとなる他のデバイスについての情報を示します。

次に、**show failover history** コマンドの出力例を示します。

```
ciscoasa(config)# show failover history
==========================================================
From State                   To State                     Reason
==========================================================
11:59:31 UTC Jan 13 2017
Active Config Applied      Active                       No Active unit found

06:17:51 UTC Jan 15 2017
Active                     Failed                       Interface check
                                                                This Host:3
                                                                  admin: inside
                                                                  ctx-1: ctx1-1
                                                                  ctx-2: ctx2-1
                                                                Other Host:0
03:58:49 UTC Feb 3 2017
Active                     Cold Standby                 Failover state check delayed due to
mate failure

03:58:51 UTC Feb 3 2017
Cold Standby               Sync Config                  Failover state check delayed due to
mate failure

03:59:18 UTC Feb 3 2017
Sync Config                Sync File System             Failover state check delayed due to
mate failure
23:11:39 UTC Jan 13 2017
Cold Standby               Failed                       HA state progression failed as
response not heard from mate

23:19:01 UTC Jan 13 2017
Sync Config                Not Detected                 HA state progression failed as
configuration sync timeout expired
 14:26:28 UTC Aug 16 2017
Standby Ready              Just Active                  Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Just Active                Active Drain                 Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Drain               Active Applying Config       Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Applying Config     Active Config Applied        Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
```

```
Active Config Applied      Active                      Inspection engine in other unit has
failed due to disk failure

18:03:35 UTC Aug 17 2017
Active                     Standby Ready               Other unit wants me Standby

18:03:36 UTC Aug 17 2017
Standby Ready              Failed                      Detect Inspection engine failure due
to disk failure

18:03:37 UTC Aug 17 2017
Failed                     Standby Ready               My Inspection engine is as good as
peer due to disk recovery
```

各エントリには、状態変更が発生した時刻および日付、開始状態、結果状態、および状態変更の理由が示されます。最も新しいエントリが表示の末尾に配置されます。古いエントリが上部に表示されます。最大で 60 エントリを表示できます。エントリが最大数に到達した場合、最も古いエントリが出力の上部から削除され、新しいエントリが末尾に追加されます。

エラーの理由には、トラブルシューティングに役立つ詳細情報が含まれています。これには、インターフェイス チェック、フェールオーバー状態チェック、状態の進行の失敗、およびサービス モジュールの失敗があります。

次に、show failover history details コマンドの出力例を示します。

```
show failover history details
==========================================================================
From State                 To State                    Reason
==========================================================================
09:58:07 UTC Jan 18 2017
Not Detected               Negotiation                 No Error

09:58:10 UTC Jan 18 2017
Negotiation                Just Active                 No Active unit found

09:58:10 UTC Jan 18 2017
Just Active                Active Drain                No Active unit found

09:58:10 UTC Jan 18 2017
Active Drain               Active Applying Config      No Active unit found

09:58:10 UTC Jan 18 2017
Active Applying Config     Active Config Applied       No Active unit found

09:58:10 UTC Jan 18 2017
Active Config Applied      Active                      No Active unit found

==========================================================================

PEER History Collected at 09:58:54 UTC Jan 18 2017
=======================PEER-HISTORY=======================================
From State                 To State                    Reason
=======================PEER-HISTORY=======================================
09:57:46 UTC Jan 18 2017
Not Detected               Negotiation                 No Error

09:58:19 UTC Jan 18 2017
Negotiation                Cold Standby                Detected an Active mate

09:58:21 UTC Jan 18 2017
Cold Standby               Sync Config                 Detected an Active mate
```

```
09:58:29 UTC Jan 18 2017
Sync Config             Sync File System              Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync File System        Bulk Sync                     Detected an Active mate

09:58:42 UTC Jan 18 2017
Bulk Sync               Standby Ready                 Detected an Active mate

========================PEER-HISTORY====================================
```

show failover history details コマンドは、ピアのフェールオーバーの履歴を要求し、ユニットのフェールオーバー履歴とピアの最新のフェールオーバー履歴を出力します。1 秒以内にピアが応答しない場合は、最後に収集されたフェールオーバー履歴情報が表示されます。

表 7-3 に、フェールオーバーの状態を示します。状態には永続的と一時的の 2 つのタイプがあります。永続的な状態とは、障害などの何らかの出来事によって状態変更が発生するまで、ユニットが維持できる状態のことです。一時的な状態とは、ユニットが永続的な状態に到達するまでの間に経過する状態です。

表 7-3　フェールオーバーの状態

States	説明
Disabled	フェールオーバーはディセーブルです。これは安定したステートです。
不合格	ユニットは障害状態です。これは安定したステートです。
Negotiation	ユニットはピアとの接続を確立し、ピアとネゴシエートして、ソフトウェア バージョンの互換性を判別し、Active/Standby ロールを決定します。ネゴシエートされたロールに基づき、ユニットはスタンバイ ユニット状態またはアクティブ ユニット状態になるか、障害状態になります。これは一時的なステートです。
Not Detected	ASA はピアの存在を検出できません。このことは、フェールオーバーがイネーブルな状態で ASA が起動されたが、ピアが存在しない、またはピアの電源がオフである場合に発生する可能性があります。
スタンバイ ユニット状態	
Cold Standby	ユニットはピアがアクティブ状態に到達するのを待機します。ピア ユニットがアクティブ状態に到達すると、このユニットは Standby Config 状態に進みます。これは一時的なステートです。
Sync Config	ユニットはピア ユニットから実行コンフィギュレーションを要求します。コンフィギュレーションの同期化中にエラーが発生した場合、ユニットは初期化状態に戻ります。これは一時的なステートです。
Sync File System	ユニットはピア システムとファイル システムを同期化します。これは一時的なステートです。
Bulk Sync	ユニットはピアから状態情報を受信します。この状態は、ステートフル フェールオーバーがイネーブルの場合にのみ発生します。これは一時的なステートです。
Standby Ready	ユニットは、アクティブ ユニットに障害が発生した場合に引き継ぐ準備が完了しています。これは安定したステートです。

表 7-3　フェールオーバーの状態(続き)

States	説明
アクティブ ユニット状態	
Just Active	ユニットがアクティブ ユニットになったときの最初の状態です。この状態にあるとき、ユニットがアクティブになること、および IP アドレスと MAC アドレスをインターフェイスに設定することをピアに通知するメッセージがピアに送信されます。これは一時的なステートです。
Active Drain	ピアからのキュー メッセージが廃棄されます。これは一時的なステートです。
Active Applying Config	ユニットはシステム コンフィギュレーションを適用します。これは一時的なステートです。
Active Config Applied	ユニットはシステム コンフィギュレーションの適用を完了しました。これは一時的なステートです。
Active	ユニットはアクティブで、トラフィックを処理しています。これは安定したステートです。

それぞれの状態変更の後に状態変更の理由が続きます。この理由は、ユニットが一時的な状態から永続的な状態に進んでも、通常同じままになります。次に、可能性がある状態変更の理由を示します。

- エラーなし
- CI config cmd によって設定されている
- フェールオーバー状態チェック
- フェールオーバー インターフェイスの準備ができた
- HELLO が受信されない
- 他のユニットのソフトウェア バージョンが異なっている
- 他のユニットの動作モードが異なっている
- 他のユニットのライセンスが異なっている
- 他のユニットのシャーシ コンフィギュレーションが異なっている
- 他のユニットのカード コンフィギュレーションが異なっている
- 他のユニットからアクティブ状態を要求された
- 他のユニットからスタンバイ状態を要求された
- 他のユニットが、このユニットに障害があるとレポートした
- 他のユニットが、そのユニットに障害があるとレポートした
- コンフィギュレーションの不一致
- アクティブ ユニットが検出された
- アクティブ ユニットが検出されなかった
- コンフィギュレーションの同期化が行われた
- 通信障害から回復した
- 他のユニットの VLAN コンフィギュレーションが異なっている

- VLAN コンフィギュレーションを確認できない
- コンフィギュレーションの同期化が不完全である
- コンフィギュレーションの同期化に失敗した
- インターフェイス チェック
- このユニットの通信が失敗した
- フェールオーバー メッセージの ACK を受信しなかった
- 同期後の学習状態で他のユニットが動作しなくなった
- ピアの電源が検出されない
- フェールオーバー ケーブルがない
- HA 状態の進行に失敗した
- サービス カード障害が検出された
- 他のユニットのサービス カードに障害が発生した
- このユニットのサービス カードはピアと同様である
- LAN インターフェイスが未設定状態になった
- ピア ユニットがリロードされた
- シリアル ケーブルから LAN ベース fover に切り替わった
- コンフィギュレーション同期化の状態を確認できない
- 自動更新要求
- 原因不明

次に、**show failover interface** コマンドの出力例を示します。デバイスのフェールオーバー インターフェイスに IPv6 アドレスが設定されています。

```
ciscoasa(config)# show failover interface
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

関連コマンド

コマンド	説明
show running-config failover	現在のコンフィギュレーション内の **failover** コマンドを表示します。

show failover exec

指定したユニットの **failover exec** コマンド モードを表示するには、特権 EXEC モードで **show failover exec** コマンドを使用します。

show failover exec {**active** | **standby** | **mate**}

構文の説明

active	アクティブ ユニットの **failover exec** コマンド モードを表示します。
mate	ピア ユニットの **failover exec** コマンド モードを表示します。
スタンバイ	スタンバイ ユニットの **failover exec** コマンド モードを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

failover exec コマンドは、指定したデバイスとのセッションを確立します。デフォルトでは、このセッションはグローバル コンフィギュレーション モードです。このセッションのコマンド モードは、**failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信することによって変更できます。指定されたデバイスの **failover exec** コマンド モードを変更しても、デバイスへのアクセスに使用しているセッションのコマンド モードは変更されません。デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。

show failover exec コマンドは、**failover exec** コマンドで送信されるコマンドが実行される、指定したデバイス上のコマンド モードを表示します。

例

次に、**show failover exec** コマンドの出力例を示します。この例では、**failover exec** コマンドが入力されるユニットのコマンド モードが、コマンドが実行される **failover exec** コマンド モードと同じである必要がないことを示しています。

この例では、スタンバイ ユニットにログインした管理者が、アクティブ ユニット上のインターフェイスに名前を追加します。この例で、**show failover exec mate** コマンドを 2 回めに入力したとき、ピア デバイスはインターフェイス コンフィギュレーション モードであると表示されます。**failover exec** コマンドでデバイスに送信されるコマンドは、このモードで実行されます。

```
ciscoasa(config)# show failover exec mate

Active unit Failover EXEC is at config mode

! The following command changes the standby unit failover exec mode
! to interface configuration mode.
ciscoasa(config)# failover exec mate interface GigabitEthernet0/1
ciscoasa(config)# show failover exec mate

Active unit Failover EXEC is at interface sub-command mode

! Because the following command is sent to the active unit, it is replicated
! back to the standby unit.
ciscoasa(config)# failover exec mate nameif test
```

関連コマンド

コマンド	説明
failover exec	フェールオーバー ペアの指定されたユニット上で、入力されたコマンドを実行します。

show file

ファイル システムに関する情報を表示するには、特権 EXEC モードで **show file** コマンドを使用します。

show file descriptors | system | information *filename*

構文の説明

descriptors	開かれているファイル記述子をすべて表示します。
filename	ファイル名を指定します。
情報	パートナー アプリケーション パッケージ ファイルなど、特定のファイルについての情報を表示します。
システム	ディスク ファイル システムについて、サイズ、利用可能なバイト数、メディアのタイプ、フラグ、およびプレフィックス情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	パートナー アプリケーション パッケージ ファイルについての情報を表示する機能が追加されました。
9.7(1)	**show file descriptor** コマンドは、システム コンテキスト モードで open ファイル記述子からだけ出力をプリントするように更新されました。

使用上のガイドライン

マルチ コンテキスト モードのシステム コンテキストで使用する場合、**show file descriptors** コマンドはすべてのコンテキストにわたって、開いている場合のファイルの記述子の詳細を表示します。コンテキストに open ファイル記述子がある場合、CLI がシステム コンテキストで実行されていれば、その特定のコンテキストの詳細のみが表示されます。システムは、「no file descriptors」のコンテキストのすべての名前は出力しません。open ファイル記述子があるコンテキストのみを表示します。

例

次に、**show firewall** コマンドの出力例を示します。

開いているファイルがない単一コンテキスト

```
ciscoasa(config)# show file descriptors
No open file descriptors
ciscoasa(config)#
```

開いているファイルがある単一のコンテキスト

```
ciscoasa(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0302  139  disk0:/test1.txt
ciscoasa(config)#
```

システム コンテキストで開いているファイルがないマルチコンテキスト

```
ciscoasa# show file descriptors
ciscoasa#
```

システム コンテキストで開いているファイルがあるマルチコンテキスト

```
ST-Campus-spyc/stby(config)# show file descriptors
Context: CTX1
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX3
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX5
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
```

ユーザ コンテキストで開いているファイルがないマルチコンテキスト

```
ST-Campus-spyc/stby/CTX1(config)# changeto context CTX2
ST-Campus-spyc/act/CTX2(config)# show file descriptors
No open file descriptors
ST-Campus-spyc/act/CTX2(config)#
```

ユーザ コンテキストで開いているファイルがあるマルチコンテキスト

```
ST-Campus-spyc/stby(config)# changeto con CTX1
ST-Campus-spyc/stby/CTX1(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
ST-Campus-spyc/stby/CTX1(config)#

ciscoasa# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

次に、**show file info** コマンドの出力例を示します。

```
ciscoasa# show file info disk0:csc_embd1.0.1000.pkg
type is package (csc)
file size is 17204149 bytes version 1
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
pwd	現在の作業ディレクトリを表示します。

show fips

FIPS のステータスを表示するには、特権 EXEC モードで **show fips** コマンドを使用します。

show fips

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが追加されました。

使用上のガイドライン

show running-configuration fips コマンドでは、FIPS が有効になったときにのみステータスが表示されていました。**show fips** コマンドは、実際の動作状態を把握するために導入されました。したがって、このコマンドでは、ユーザが無効または有効状態になっている FIPS を有効または無効にするときに、FIPS ステータスが表示されます。また、このコマンドで、アクションを有効化または無効化した後でデバイスを再起動するためのステータスも表示されます。

例

次に、**show fips** コマンドの出力例を示します。

FIPS が無効になっていて、ユーザが **fips enable** を実行してこれを有効にすると、次のようになります。

```
ciscoasa# show fips
FIPS is currently disabled and will be enabled after reboot
```

ASA のリブート後、

```
ciscoasa# show fips
FIPS is currently enabled
```

FIPS が有効になっていて、ユーザが **no fips enable** を実行してこれを無効にすると、次のようになります。

```
ciscoasa# show fips
FIPS is currently enabled and will be disabled after reboot
```

ASA のリブート後、

```
ciscoasa# show fips
FIPS is currently disabled
```

FIPS が無効になっていて、ユーザが **no fips enable** を実行してこれを無効にすると、次のようになります。

```
ciscoasa# show fips
FIPS is currently disabled
```

FIPS が有効になっていて、ユーザが **fips enable** を実行してこれを有効にすると、次のようになります。

```
ciscoasa# show fips
FIPS is currently enabled
```

関連コマンド

コマンド	説明
fips enable	ASA で FIPS を有効にします。
show running-configuration fips	fips の現在の実行コンフィギュレーションと動作コンフィギュレーションを表示します。

show firewall

現在のファイアウォール モード(ルーテッドまたはトランスペアレント)を表示するには、特権 EXEC モードで **show firewall** コマンドを使用します。

show firewall

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show firewall** コマンドの出力例を示します。

```
ciscoasa# show firewall
Firewall mode: Router
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを設定します。
show mode	現在のコンテキスト モード(シングルまたはマルチ)を表示します。

show flash

内部フラッシュ メモリの内容を表示するには、特権 EXEC モードで **show flash:** コマンドを使用します。

show flash: all | controller | filesys

(注) ASA では、**flash** キーワードにエイリアス **disk0** が使用されます。

構文の説明

all	すべてのフラッシュの情報を表示します。
コントローラ	ファイル システム コントローラの情報を表示します。
filesys	ファイル システムの情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show flash:** コマンドの出力例を示します。

```
ciscoasa# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
```

```
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
show disk0:	内部フラッシュ メモリの内容を表示します。
show disk1:	外部フラッシュ メモリ カードの内容を表示します。

show flow-export counters

NetFlow データに関連付けられているランタイム カウンタを表示するには、特権 EXEC モードで **show flow-export counters** コマンドを使用します。

show flow-export counters

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。
9.0(1)	送信元ポート割り当ての失敗に対する新しいエラー カウンタが追加されました。

使用上のガイドライン

ランタイム カウンタには、統計データおよびエラー データが含まれます。

例

次に、NetFlow データに関連付けられているランタイム カウンタを表示する **show flow-export counters** コマンドの出力例を示します。

```
ciscoasa# show flow-export counters

destination: inside 209.165.200.224 2055
 Statistics:
  packets sent                      1000
 Errors:
  block allocation failure             0
  invalid interface                    0
  template send failure                0
  no route to collector                0
  source port allocation               0
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。

show flow-offload

フロー オフロードについての情報を表示するには、特権 EXEC モードで **show flow-offload** コマンドを使用します。

show flow-offload {**info** [**detail**] | **cpu** | **flow** [**count** | **detail**] | **statistics**}

構文の説明

info [**detail**]	オフロード エンジンに関する基本情報を表示します。ポートの使用状況の要約などの追加情報を取得するには、**detail** キーワードを追加します。
cpu	オフロード コアの負荷のパーセンテージを表示します。
flow [**count**	**detail**]	オフロードされているアクティブなフローに関する情報を表示します。オプションで次のキーワードを追加できます。 • **count**：オフロードされているアクティブなフローと作成済みのオフロードされたフローの数を表示します。 • **detail**：オフロードされているアクティブなフローとそれらの書き換えルールとデータを表示します。
statistics	オフロードされたフローのパケット統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが導入されました。

使用上のガイドライン

フロー オフロードが有効な場合は、このコマンドを使用して、サービスとオフロードされたフローに関する情報を表示できます。

例

次に、**show flow-offload statistics** コマンドの出力例を示します。出力には、送信（Tx）パケット数、受信（Rx）パケット数、ドロップされたパケット数、および使用された仮想 NIC（VNIC）の統計情報が示されます。

```
ciscoasa# show offload-engine statistics
Packet stats of port : 0
        Tx Packet count                 :        785807566
        Rx Packet count                 :        785807566
        Dropped Packet count            :                0
        VNIC transmitted packet         :        785807566
        VNIC transmitted bytes          :     103726598712
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
 Packet stats of port : 1
        Tx Packet count                 :                0
        Rx Packet count                 :                0
        Dropped Packet count            :                0
        VNIC transmitted packet         :                0
        VNIC transmitted bytes          :                0
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
```

関連コマンド

コマンド	説明
clear flow-offload	オフロード統計情報またはフローをクリアします。
flow-offload	フロー オフロードを有効にします。
set-connection advanced-options flow-offload	オフロードの対象としてトラフィック フローを指定します。

show fragment

IP フラグメント再構築モジュールの動作データを表示するには、特権 EXEC モードで **show fragment** コマンドを使用します。

show fragment [*interface*]

構文の説明

interface	（任意）ASA のインターフェイスを指定します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーション データと動作データを分けるために、**show fragment** および **show running-config fragment** の 2 つのコマンドに分けられました。

例

次に、IP フラグメント再構築モジュールの動作データを表示する方法の例を示します。

```
ciscoasa# show fragment
Interface: outside
Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 8, Overflow: 74
```

それぞれの説明は次のとおりです。

- サイズ（Size）：IP 再構築データベース内で再構築を待機可能な最大フラグメント数を設定します。デフォルトは 200 です。**注**：このデータベースは、インターフェイスごとに存在します。
- チェーン（Chain）：完全な IP パケットをフラグメント化する場合の最大フラグメント数を指定します。デフォルトは 24 です。
- タイムアウト（Timeout）：フラグメント化されたパケット全体が到着するのを待機する最大秒数を指定します。デフォルトは 5 秒です。
- リアセンブル（Reassembly）：仮想（virtual）または完全（full）。デフォルトは virtual です。IP フラグメントが ASA で終了する場合やアプリケーション レベルでインスペクションを必要とする場合には、完全（物理的）にリアセンブルされます。必要に応じて、完全（物理的）にリアセンブルされたパケットは、出力インターフェイスで再度フラグメント化できます。

- キュー(Queue):リアセンブル データベースで現在リアセンブルを待機しているフラグメントの数。注:ASA では、リアセンブル データベースのサイズが、設定されている最大リアセンブル データベース サイズの 2/3 に達すると、既存のフラグメント チェーンに含まれていない新しいフラグメントが許可されなくなります。過剰なフラグメントが廃棄された場合に、この状況についての syslog メッセージは生成されません。
- 構成済(Assembled):完全にリアセンブルされた(フラグメントではない)IP パケットの数。仮想リアセンブルがパケットに適用された場合、この数は増やされません。
- 失敗(Fail):リアセンブルに失敗した(フラグメントではない)IP パケットの数。たとえば、着信パケットが "chain" のフラグメント数よりも多くフラグメント化された場合、この数が増やされます。この場合は、syslog メッセージ 209005 が生成されます(デフォルトでは、10 秒当たり 1 メッセージにレート制限されます)。
- オーバーフロー(Overflow):リアセンブル データベースでオーバーフローしたフラグメント数。これらのフラグメントは破棄されます。リアセンブル データベースの最大サイズに到達して、新しいフラグメントが到着した場合、syslog メッセージ 209003 が生成されます(デフォルトでは、10 秒当たり 1 メッセージにレート制限されます)。

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

show fxos mode

アプライアンスモードまたはプラットフォームモードの Firepower 2100 を表示するには、特権 EXEC モードで **show fxos mode** コマンドを使用します。

show fxos mode

(注) このコマンドは Firepower 2100 のみでサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、モードはアプライアンスモードに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

Firepower 2100 は、Firepower eXtensible Operating System（FXOS）という基礎となるオペレーティング システムを実行します。Firepower 2100 は、次のモードで実行できます。

- アプライアンスモード（デフォルト）：アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。
- プラットフォーム モード：プラットフォーム モードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Firepower Chassis Manager Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。

現在のモードを表示するには、**show fxos mode** を使用します。

例

次に、**show fxos mode** コマンドの出力例を示します。

```
ciscoasa# show fxos mode
Mode is currently set to appliance
```

関連コマンド

コマンド	説明
connect fxos	FXOS CLI に接続します。
fxos mode appliance	モードをアプライアンスモードに設定します。

show gc

ガーベッジ コレクション プロセスの統計情報を表示するには、特権 EXEC モードで **show gc** コマンドを使用します。

show gc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show gc** コマンドの出力例を示します。

```
ciscoasa# show gc

Garbage collection process stats:
Total tcp conn delete response             :           0
Total udp conn delete response             :           0
Total number of zombie cleaned             :           0
Total number of embryonic conn cleaned     :           0
Total error response                       :           0
Total queries generated                    :           0
Total queries with conn present response   :           0
Total number of sweeps                     :         946
Total number of invalid vcid               :           0
Total number of zombie vcid                :           0
```

関連コマンド

コマンド	説明
clear gc	ガーベッジ コレクション プロセスの統計情報を削除します。

show h225

ASA を越えて確立された H.225 セッションの情報を表示するには、特権 EXEC モードで **show h225** コマンドを使用します。

show h225

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show h225 コマンドは、ASA を越えて確立されている H.225 セッションの情報を表示します。

show h225、**show h245**、または **show h323 ras** コマンドを使用する前に、**pager** コマンドを設定することを推奨します。セッション レコードが多いときに **pager** コマンドが設定されていない場合、**show** コマンドの出力が末端に届くまでに時間がかかる場合があります。

異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値に基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

例

次に、**show h225** コマンドの出力例を示します。

```
ciscoasa# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

この出力は、ローカル エンドポイント 10.130.56.3 と外部ホスト 172.30.254.203 との間で ASA を通過するアクティブな H.323 コールが 1 つ存在し、これらのエンドポイントの間には、コールの CRV（Call Reference Value）が 9861 の同時コールが 1 つ存在することを示しています。

ローカル エンドポイント 10.130.56.4 と外部ホスト 172.30.254.205 については、同時コールの数は 0 です。つまり H.225 セッションがまだ存在しているものの、このエンドポイント間にはアクティブ コールがないことを意味します。この状況は、**show h225** コマンドを実行したときに、コールはすでに終了しているが、H.225 セッションがまだ削除されていない場合に発生する可能性があります。または、2 つのエンドポイントが、「maintainConnection」を TRUE に設定しているため、TCP 接続をまだ開いたままにしていることを意味する可能性もあります。したがって、「maintainConnection」を再度 FALSE に設定するまで、またはコンフィギュレーション内の H.225 タイムアウト値に基づくセッションのタイムアウトが起こるまで、セッションは開いたままになります。

関連コマンド

コマンド	説明
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによって ASA 間で確立された H.245 セッションの情報を表示します。
show h323 ras	ASA 間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show h245

スロー スタートを使用しているエンドポイントが ASA を越えて確立した H.245 セッションの情報を表示するには、特権 EXEC モードで **show h245** コマンドを使用します。

show h245

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show h245 コマンドは、スロー スタートを使用しているエンドポイントが ASA を越えて確立した H.245 セッションの情報を表示します。(スロー スタートでは、コールの 2 つのエンドポイントが H.245 用に別の TCP コントロール チャネルを開きます。ファスト スタートは、H.245 メッセージが H.225 コントロール チャネルで H.225 メッセージの一部として交換された場合です。

例

次に、**show h245** コマンドの出力例を示します。

```
ciscoasa# show h245
Total: 1
        LOCAL            TPKT    FOREIGN          TPKT
1       10.130.56.3/1041         0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

ASA でアクティブな H.245 コントロール セッションが、現在 1 つあります。ローカル エンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。(TKTP ヘッダーは、各 H.225/H.245 メッセージの先頭の 4 バイト ヘッダーです。このヘッダーで、この 4 バイトのヘッダーを含むメッセージの長さがわかります)。外部のホストのエンドポイントは、172.30.254.203 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。

これらのエンドポイント間でネゴシエートされるメディアは、論理チャネル番号(LCN)が 258 で、外部の RTP IP アドレス/ポート ペアが 172.30.254.203/49608、RTCP IP アドレス/ポートが 172.30.254.203/49609、ローカルの RTP IP アドレス/ポート ペアが 10.130.56.3/49608、RTCP ポートが 49609 です。

値が 259 の 2 番めの LCN は、外部の RTP IP アドレス/ポート ペアが 172.30.254.203/49606、RTCP IP アドレス/ポート ペアが 172.30.254.203/49607、ローカルの RTP IP アドレス/ポート ペアが 10.130.56.3/49606、RTCP ポートが 49607 です。

関連コマンド

コマンド	説明
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによって ASA 間で確立された H.245 セッションの情報を表示します。
show h323 ras	ASA 間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show h323

H.323 接続の情報を表示するには、特権 EXEC モードで **show h323** コマンドを使用します。

show h323 {ras | gup}

構文の説明

ras	ASA を越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションを表示します。
gup	H323 ゲートウェイ アップデート プロトコル接続に関する情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show h323 ras コマンドは、ASA を越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの情報を表示します。

例

次に、**show h323 ras** コマンドの出力例を示します。

```
ciscoasa# show h323 ras
ciscoasa#
Total: 1
        GK                      Caller
        172.30.254.214 10.130.56.14
```

この出力は、ゲートキーパー 172.30.254.214 とそのクライアント 10.130.56.14 の間にアクティブな登録が 1 つあることを示しています。

関連コマンド

コマンド	説明
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによって ASA 間で確立された H.245 セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show hardware-bypass

ISA 3000上の現在のハードウェア バイパスのステータスを表示するには、特権 EXEC モードで **show hardware-bypass** コマンドを使用します。

show hardware-bypass

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	—	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1.225)	このコマンドが追加されました。

例

次に、**show hardware-bypass** コマンドの出力例を示します。

```
ciscoasa# show hardware-bypass
                          Status              Powerdown           Powerup
GigabitEthernet 1/1-1/2   Disable             Disable             Disable
GigabitEthernet 1/3-1/4   Disable             Disable             Disable

Pairing supported on these interfaces: gig1/1 & gig1/2, gig1/3 & gig1/4
```

関連コマンド

コマンド	説明
hardware-bypass	ISA 3000 デバイスでハードウェア バイパス モードを設定します。

show history

以前入力したコマンドを表示するには、ユーザ EXEC モードで **show history** コマンドを使用します。

show history

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show history コマンドを使用すると、以前入力したコマンドを表示できます。上矢印と下矢印を使用してコマンドを個別に調べて、**^p** を入力して以前に入力した行を表示するか、**^n** を入力して次の行を表示できます。

例

次に、ユーザ EXEC モードで **show history** コマンドを使用する例を示します。

```
ciscoasa> show history
    show history
    help
    show history
```

次に、特権 EXEC モードで **show history** コマンドを使用する例を示します。

```
ciscoasa# show history
    show history
    help
    show history
    enable
    show history
```

次に、グローバル コンフィギュレーション モードで **show history** コマンドを使用する例を示します。

```
ciscoasa(config)# show history
    show history
    help
    show history
    enable
    show history
    config t
    show history
```

関連コマンド

コマンド	説明
help	指定したコマンドのヘルプ情報を表示します。

show hostname

ホスト名を表示するには、特権 EXEC モードで **show hostname** コマンドを使用します。

show hostname [**fqdn**]

構文の説明

fqdn	完全修飾ドメイン名を表示します。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォールモード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	コマンドが追加されました。

使用上のガイドライン

hostname コマンドを使用してホスト名を設定し、**domain-name** コマンドを使用してドメインを設定します。

例

次に、show hostname fqdn コマンドの出力例を示します。

```
ciscoasa# show hostname fqdn
asa1.cisco.com
```

関連コマンド

コマンド	説明
hostname	ASA のホスト名を設定します。
domain-name	ASA のドメイン名を設定します。

show icmp

ICMP コンフィギュレーションを表示するには、特権 EXEC モードで **show icmp** コマンドを使用します。

show icmp

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはすでに存在していました。

使用上のガイドライン

show icmp コマンドは ICMP コンフィギュレーションを表示します。

例

次に、ICMP コンフィギュレーションを表示する例を示します。

```
ciscoasa# show icmp
```

関連コマンド

clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
icmp	ASA インターフェイスが終端となる ICMP トラフィックのアクセス ルールを設定します。
inspect icmp	ICMP インスペクション エンジンをイネーブルまたはディセーブルにします。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show idb

Interface Descriptor Block のステータスについての情報を表示するには、特権 EXEC モードで **show idb** コマンドを使用します。

show idb

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

IDB はインターフェイス リソースを表す内部データ構造です。出力の説明については、「例」を参照してください。

例

次に、**show idb** コマンドの出力例を示します。

```
ciscoasa# show idb
Maximum number of Software IDBs 280. In use 23.

                    HWIDBs     SWIDBs
              Active 6          21
            Inactive 1          2
          Total IDBs 7          23
 Size each (bytes) 116        212
        Total bytes 812        4876

HWIDB#  1 0xbb68ebc  Control0/0
HWIDB#  2 0xcd47d84  GigabitEthernet0/0
HWIDB#  3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#  4 0xcd5063c  GigabitEthernet0/2
HWIDB#  5 0xcd54a9c  GigabitEthernet0/3
HWIDB#  6 0xcd58f04  Management0/0
```

```
SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

表 7-4 に、各フィールドの説明を示します。

表 7-4　show idb stats の各フィールド

フィールド	説明
HWIDBs	すべての HWIDB の統計情報を表示します。HWIDB は、システム内の各ハードウェア ポートについて作成されます。
SWIDBs	すべての SWIDB の統計情報を表示します。SWIDB は、システム内の各メインおよびサブインターフェイスについて、およびコンテキストに割り当てられている各インターフェイスについて作成されます。 他の一部の内部ソフトウェア モジュールも IDB を作成します。
HWIDB#	ハードウェア インターフェイス エントリを示します。IDB シーケンス番号、アドレス、およびインターフェイス名が各行に表示されます。
SWIDB#	ソフトウェア インターフェイス エントリを示します。IDB シーケンス番号、アドレス、対応する vPif ID、およびインターフェイス名が各行に表示されます。
PEER IDB#	コンテキストに割り当てられているインターフェイスを示します。IDB シーケンス番号、アドレス、対応する vPif ID、コンテキスト ID、およびインターフェイス名が各行に表示されます。

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show igmp groups

ASA に直接接続された受信者、および IGMP によって学習された受信者を含むマルチキャスト グループを表示するには、特権 EXEC モードで **show igmp groups** コマンドを使用します。

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

構文の説明

detail	(任意) ソースの詳細説明を出力します。
group	(任意) IGMP グループのアドレス。このオプション引数を含めると、表示は指定されたグループに限定されます。
if_name	(任意) 指定されたインターフェイスについてのグループ情報を表示します。
reserved	(任意) 予約されたグループについての情報を表示します。
summary	(任意) グループ加入の要約情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

オプションの引数およびキーワードをすべて省略すると、**show igmp groups** コマンドは、直接接続されたマルチキャスト グループを、グループ アドレス、インターフェイス タイプ、およびインターフェイス番号別に表示します。

例

次に、**show igmp groups** コマンドの出力例を示します。

```
ciscoasa# show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

show igmp interface

インターフェイスのマルチキャスト情報を表示するには、特権 EXEC モードで **show igmp interface** コマンドを使用します。

show igmp interface [*if_name*]

構文の説明

if_name	（任意）選択したインターフェイスについての IGMP グループ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。**detail** キーワードが削除されました。

使用上のガイドライン

オプションの *if_name* 引数を省略すると、**show igmp interface** コマンドはすべてのインターフェイスについての情報を表示します。

例

次に、**show igmp interface** コマンドの出力例を示します。

```
ciscoasa# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

関連コマンド

コマンド	説明
show igmp groups	ASA に直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャスト グループを表示します。

show igmp traffic

IGMP トラフィックの統計情報を表示するには、特権 EXEC モードで **show igmp traffic** コマンドを使用します。

show igmp traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show igmp traffic** コマンドの出力例を示します。

```
ciscoasa# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                              Received     Sent
Valid IGMP Packets               3           6
Queries                          2           6
Reports                          1           0
Leaves                           0           0
Mtrace packets                   0           0
DVMRP packets                    0           0
PIM packets                      0           0

Errors:
Malformed Packets                0
Martian source                   0
Bad Checksums                    0
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP 統計カウンタをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

show import webvpn

ASA または Anyconnect セキュア モビリティ クライアントをカスタマイズおよびローカライズする、フラッシュ メモリ内のファイル、カスタマイゼーション オブジェクト、変換テーブル、またはプラグインを一覧表示するには、特権 EXEC モードで **show import webvpn** コマンドを使用します。

show import webvpn {**AnyConnect-customization** | **customization** | **mst-translation** | **plug-in** | **translation-table** | **url-list** | **webcontent**}[**detailed** | **xml-output**]

構文の説明

AnyConnect-customization	AnyConnect クライアント GUI をカスタマイズする、ASA フラッシュ メモリ内のリソース ファイル、実行可能ファイルおよび MS トランスフォームを表示します。
カスタマイゼーション	クライアントレス VPN ポータルをカスタマイズする、ASA フラッシュ メモリ内の XML カスタマイゼーション オブジェクトを表示します(ファイル名は base64 デコード済み)。
mst-translation	AnyConnect クライアント インストーラ プログラムを翻訳する、ASA フラッシュ メモリ内の MS トランスフォームを表示します。
plug-in	ASA フラッシュ メモリ内のプラグイン モジュールを表示します(SSH、VNC、および RDP などのサードパーティの Java ベースのクライアント アプリケーション)。
translation-table	クライアントレス ポータル、Secure Desktop およびプラグインによって表示されるユーザ メッセージの言語を変換する、ASA フラッシュ メモリ内の変換テーブルを表示します。
url-list	クライアントレス ポータルによって使用される、ASA フラッシュ メモリ内の URL の一覧を表示します(ファイル名は base64 デコード済み)。
webcontent	クライアントレス ポータル、クライアントレス アプリケーションおよびプラグインによって、エンド ユーザに表示されるオンライン ヘルプに使用される、ASA フラッシュ メモリ内のコンテンツを表示します。
detailed	フラッシュ メモリ内のファイルおよびハッシュのパスを表示します。
xml-output	ファイルの XML を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	**AnyConnect-customization** キーワードが追加されました。

使用上のガイドライン

show import webvpn コマンドを使用すると、クライアントレス SSL VPN ユーザが使用可能なカスタム データおよび Java ベースのクライアント アプリケーションが識別されます。表示されるリストでは、ASA のフラッシュ メモリにある要求されるすべてのデータ タイプの詳細が表示されます。

Example

次に、さまざまな **show import webvpn** コマンドによって表示される WebVPN データの例を示します。

```
ciscoasa# show import webvpn plug
ssh
rdp
vnc
ciscoasa#

ciscoasa#show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tue, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTsPnjdBOo= Tue, 15 Sep 2009 23:23:56 GMT
rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT
ciscoasa# show import webvpn customization
Template
DfltCustomization
ciscoasa#

ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                              customization
  ua                                              customization
ciscoasa#

ciscoasa# show import webvpn url-list
Template
```

```
No bookmarks are currently defined
ciscoasa#

ciscoasa# show import webvpn webcontent
No custom webcontent is loaded
ciscoasa#
```

関連コマンド

コマンド	説明
revert webvpn all	ASA に現在存在するすべての WebVPN データおよびプラグインを削除します。

show interface

インターフェイス統計情報を表示するには、特権 EXEC モードで **show interface** コマンドを使用します。

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number* | **vni** *id* [**summary**]] [**stats** | **detail**]

構文の説明

detail	(任意)インターフェイスの詳細な情報を表示します。この情報には、インターフェイスが追加された順序、設定されている状態、実際の状態、非対称ルーティングの統計情報(**asr-group** コマンドによって非対称ルーティングがイネーブルになっている場合)が含まれます。すべてのインターフェイスを表示すると、SSM の内部インターフェイスが ASA 5500 にインストールされている場合は、それらのインターフェイスに関する情報が表示されます。内部インターフェイスは、ユーザによる設定は不可能です。情報はデバッグだけを目的としています。
interface_name	(任意)**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	(任意)**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	(任意)**gigabitethernet 0/1** のようなインターフェイス ID を識別します。有効値については、**interface** コマンドを参照してください。
redundant*number*	(任意)**redundant1** のような冗長インターフェイス ID を識別します。
stats	(デフォルト)インターフェイス情報および統計情報を表示します。このキーワードはデフォルトであるため、このキーワードはオプションです。
summary	(オプション)VNI インターフェイスの場合は、VNI インターフェイスのパラメータのみを表示します。
サブインターフェイス	(任意)論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	(オプション)Firepower 1010、ASA 5505、または ASASM の場合に、VLAN インターフェイスを指定します。
vni *id*	(オプション)VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。

デフォルト

いずれのオプションも識別しない場合、このコマンドはすべてのインターフェイスについての基本的な統計情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいインターフェイス番号付け方式を取り入れるように変更され、明示的に指定するための **stats** キーワード、および **detail** キーワードが追加されました。
7.0(4)	4GE SSM インターフェイスのサポートが追加されました。
7.2(1)	スイッチ インターフェイスのサポートが追加されました。
8.0(2)	冗長インターフェイスのサポートが追加されました。また、サブインターフェイス用の遅延が追加されました。入力リセット ドロップと出力リセット ドロップの 2 つの新しいカウンタが追加されました。
8.2(1)	No buffer の数値が、ブロック割り当てからの失敗の数を示すように変更されました。
8.6(1)	ASA 5512-X ～ ASA 5555-X の共有管理インターフェイス、およびソフトウェア モジュールのコントロール プレーン インターフェイスのサポートが追加されました。管理インターフェイスは **show interface detail** コマンドを使用して Internal-Data0/1 として表示され、コントロール プレーン インターフェイスは Internal-Control0/0 として表示されます。
9.4(1)	**vni** インターフェイス タイプが追加されました。
9.5(1)	クラスタリング サイト固有の MAC アドレスが出力に追加されました。
9.10(1)	Firepower 2100/4100/9300 の場合、コマンドの出力は、インターフェイスのスーパーバイザの関連付けステータスを表示するために強化されています。
9.13(1)	アプライアンスモードでの Firepower 1000 シリーズおよび Firepower 2100 のサポートが追加されました。

使用上のガイドライン

1 つのインターフェイスが複数のコンテキストで共有されているときに、あるコンテキストでこのコマンドを入力した場合、ASA は現在のコンテキストの統計情報だけを表示します。物理インターフェイスのシステム実行スペース内でこのコマンドを使用すると、ASA はすべてのコンテキストについて組み合わせた統計情報を表示します。

サブインターフェイスについて表示される統計情報の数は、物理インターフェイスについて表示される統計情報の数のサブセットです。

インターフェイス名は、システム実行スペースでは使用できません。これは、**nameif** コマンドはコンテキスト内だけで使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内だけで使用できます。**allocate-interface** コマンドで **visible** キーワードを設定した場合、ASA は **show interface** コマンドの出力にインターフェイス ID を表示します。

(注) Hardware カウントと Traffic Statistics カウントでは、送信または受信されるバイト数が異なります。

Hardware カウントでは、この量はハードウェアから直接取得され、レイヤ 2 パケットのサイズが反映されます。一方、Traffic Statistics では、レイヤ 3 パケットのサイズが反映されます。

カウントの差はインターフェイス カード ハードウェアの設計に基づいて異なります。

たとえば、ファスト イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーを含むため、トラフィック カウントよりも 14 バイト大きくなります。ギガビット イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーと CRC の両方を含むため、トラフィック カウントよりも 18 バイト大きくなります。

出力の説明については、「例」を参照してください。

例

次に、**show interface** コマンドの出力例を示します。

```
ciscoasa# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
```

```
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Active member of Redundant5
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
```

```
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max packets): hardware (128/128) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
        Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c451, MTU 1500
        IP address 10.2.3.5, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

次の出力は、使用している場合のサイト MAC アドレスの使用状況を示しています。

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
    Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 3151
        MAC address aaaa.1111.1234, MTU 1500
        Site Specific MAC address aaaa.1111.aaaa
        IP address 10.3.1.1, subnet mask 255.255.255.0
    Traffic Statistics for "inside":
        132269 packets input, 6483425 bytes
        1062 packets output, 110448 bytes
        98530 packets dropped
```

表 7-5 に、各フィールドの説明を示します。

表 7-5　show interface の各フィールド

フィールド	説明
Interface *ID*	インターフェイス ID。コンテキスト内では、**allocate-interface** コマンドで **visible** キーワードを設定しない限り、ASA はマッピング名（設定されている場合）を表示します。
"*interface_name*"	**nameif** コマンドで設定されたインターフェイス名。システム実行スペースでは、システムに名前を設定できないため、このフィールドはブランクです。名前を設定しない場合、Hardware 行の下に次のメッセージが表示されます。 `Available but not configured via nameif`
is *state*	管理ステートは次のとおりです。 • up：インターフェイスはシャットダウンされません。 • administratively down：インターフェイスは、**shutdown** コマンドを使用してシャットダウンされます。
Line protocol is *state*	回線ステータスは次のとおりです。 • up：動作するケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。
VLAN 識別子	サブインターフェイスの場合、VLAN ID。
ハードウェア	インターフェイスのタイプ、最大帯域幅、遅延、デュプレックス方式、および速度。リンクがダウンしている場合は、デュプレックス方式と速度は設定値が表示されます。リンクが動作している場合、これらのフィールドには実際の設定がカッコで囲まれて設定値とともに表示されます。次に、一般的なハードウェア タイプを示します。 • i82542：PIX プラットフォームで使用される Intel PCI ファイバ ギガビット カード • i82543：PIX プラットフォームで使用される Intel PCI-X ファイバ ギガビット カード • i82546GB：ASA プラットフォーム上で使用される Intel PCI-X 銅線ギガビット • i82547GI：ASA プラットフォーム上でバックプレーンとして使用される Intel CSA 銅線ギガビット • i82557：ASA プラットフォーム上で使用される Intel PCI 銅線ファスト イーサネット • i82559：PIX プラットフォームで使用される Intel PCI 銅線ファスト イーサネット • VCS7380：SSM-4GE で使用される Vitesse 4 ポート ギガビット スイッチ
Media-type	（4GE SSM インターフェイスの場合のみ）インターフェイスが RJ-45 または SFP のいずれとして設定されているかを示します。

表 7-5　show interface の各フィールド(続き)

フィールド	説明

message area	一部の状況で、メッセージが表示される場合もあります。次の例を参照してください。
	• システム実行スペースで、次のメッセージが表示される場合があります。
	`Available for allocation to a context`
	• 名前を設定しない場合、次のメッセージが表示されます。
	`Available but not configured via nameif`
	• インターフェイスが冗長インターフェイスのメンバの場合、次のメッセージが表示されます。
	`Active member of Redundant5`

MAC address	インターフェイスの MAC アドレス。
Site Specific MAC address	クラスタリングの場合に、使用中のサイト固有の MAC アドレスを表示します。
MTU	このインターフェイス上で許可されるパケットの最大サイズ(バイト単位)。インターフェイス名を設定しない場合、このフィールドには「MTU not set」と表示されます。
IP address	**ip address** コマンドを使用して設定したか、DHCP サーバから受信したインターフェイスの IP アドレス。システム実行スペースでは、システムに IP アドレスを設定できないため、このフィールドには「IP address unassigned」と表示されます。
サブネット マスク	IP アドレスのサブネット マスク。
Packets input	このインターフェイスで受信したパケットの数。
Bytes	このインターフェイスで受信したバイト数。
No buffer	ブロック割り当てからの失敗の数。
Received:	
Broadcasts	受信したブロードキャストの数。
Input errors	次に示すタイプを含めた入力エラーの総数。入力に関係する他のエラーも入力エラーのカウントが増加する原因になります。また、一部のデータグラムは複数のエラーを含んでいることもあります。したがって、この合計数は、次に示すタイプについて表示されるエラーの数を超えることがあります。
Runts	最小のパケット サイズ(64 バイト)よりも小さいために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。
Giants	最大パケット サイズを超えたため廃棄されるパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。

表 7-5　show interface の各フィールド(続き)

フィールド	説明
CRC	巡回冗長検査エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、ASA は CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。
Frame	フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。
Overrun	ASA のデータ処理能力を入力レートが超えたため、ASA がハードウェア バッファに受信したデータを処理できなかった回数。
Ignored	このフィールドは使用されません。値は常に 0 です。
中断	このフィールドは使用されません。値は常に 0 です。
L2 decode drops	名前がまだ設定されていないか(**nameif** コマンド)、無効な VLAN ID を持つフレームが受信されたためにドロップしたパケットの数。冗長インターフェイス コンフィギュレーションのスタンバイ インターフェイスでは、このインターフェイスに名前(**nameif コマンド**)が設定されていないため、カウンタが増加する可能性があります。
Packets output	このインターフェイスに送信されたパケットの数。
Bytes	このインターフェイスに送信されたバイトの数。
Underruns	ASA が処理できるよりも速くトランスミッタが稼働した回数。
Output Errors	設定されたコリジョンの最大数を超えたため送信されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。
Collisions	イーサネット コリジョン(単一および複数のコリジョン)が原因で再送信されたメッセージの数。これは通常、過渡に延長した LAN で発生します(イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間のリピータが 2 つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合)。衝突するパケットは、出力パケットによって 1 回だけカウントされます。
Interface resets	インターフェイスがリセットされた回数。インターフェイスで 3 秒間送信できない場合、ASA はインターフェイスをリセットして送信を再開します。この間隔では、接続状態が維持されます。インターフェイスのリセットは、インターフェイスがループバックまたはシャットダウンする場合も発生します。
Babbles	未使用。(「バブル」は、トランスミッタが最長フレームの送信に要した時間よりも長くインターフェイスに留まっていたことを意味します)。

表 7-5　show interface の各フィールド(続き)

フィールド	説明
Late collisions	通常のコリジョン ウィンドウの外側でコリジョンが発生したため、送信されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2 つのイーサネット ホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2 番めのホストが 1 番めのホストの通信状態を確認して待機します。 レイト コリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、ASA はパケットの送信を部分的に完了しています。ASA は、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネット ネットワークです。
Deferred	リンク上のアクティビティが原因で送信前に保留されたフレームの数。
input reset drops	リセットが発生したときに RX リングでドロップしたパケットの数をカウントします。
output reset drops	リセットが発生したときに TX リングでドロップしたパケットの数をカウントします。
Rate limit drops	(4GE SSM インターフェイスの場合だけ)ギガビット以外の速度でインターフェイスを設定して、設定に応じて 10 Mbps または 100 Mbps を超えて送信しようとした場合にドロップされたパケットの数。
Lost carrier	送信中に搬送波信号が消失した回数。
No carrier	未使用。
Input queue (curr/max packets):	入力キュー内のパケットの数(現行値と最大値)。
ハードウェア	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。ギガビット イーサネット インターフェイスでは使用できません。
Output queue (curr/max packets):	出力キュー内のパケットの数(現行値と最大値)。
ハードウェア	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。
input queue (blocks free curr/low)	curr/low エントリは、インターフェイスの受信(入力)記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メイン CPU によって更新されるため、all-time-lowest(インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで)の水準点はあまり正確ではありません。

表 7-5　show interface の各フィールド(続き)

フィールド	説明
output queue (blocks free curr/low)	curr/low エントリは、インターフェイスの送信(出力)記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メイン CPU によって更新されるため、all-time-lowest(インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで)の水準点はあまり正確ではありません。
Traffic Statistics:	受信、送信、またはドロップしたパケットの数。
Packets input	受信したパケットの数とバイトの数。
Packets output	送信したパケットの数とバイトの数。
Packets dropped	ドロップしたパケットの数。このカウンタは通常、高速セキュリティ パス(ASP)上でドロップしたパケットについて増分します(たとえば、アクセスリスト拒否が原因でパケットをドロップした場合など)。 インターフェイス上でドロップが発生する原因については、**show asp drop** コマンドを参照してください。
1 minute input rate	過去 1 分間に受信したパケットの数(パケット/秒およびバイト/秒)。
1 minute output rate	過去 1 分間に送信したパケットの数(パケット/秒およびバイト/秒)。
1 minute drop rate	過去 1 分間にドロップしたパケットの数(パケット/秒)。
5 minute input rate	過去 5 分間に受信したパケットの数(パケット/秒およびバイト/秒)。
5 minute output rate	過去 5 分間に送信したパケットの数(パケット/秒およびバイト/秒)。
5 minute drop rate	過去 5 分間にドロップしたパケットの数(パケット/秒)。
Redundancy Information:	冗長インターフェイスについて、メンバー物理インターフェイスを示します。アクティブ インターフェイスの場合はインターフェイス ID の後に「(Active)」と表示されます。 メンバーをまだ割り当てていない場合、次の出力が表示されます。 `Members unassigned`
Last switchover	冗長インターフェイスの場合、アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした時刻を表示します。

次に、スイッチ ポートを含む ASA 5505 上での **show interface** コマンドの出力例を示します。

```
ciscoasa# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
```

```
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec,  0 bytes/sec
  5 minute output rate 0 pkts/sec,  0 bytes/sec
  5 minute drop rate, 0 pkts/sec

Interface Ethernet0/0 "", is up, line protocol is up
  Hardware is 88E6095, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        Available but not configured via nameif
        MAC address 00d0.2bfd.6ec5, MTU not set
        IP address unassigned
        407 packets input, 53587 bytes, 0 no buffer
        Received 103 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        43 switch ingress policy drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        0 rate limit drops
        0 switch egress policy drops
```

表 7-7 に、Firepower 1010 または ASA 5505 のスイッチインターフェイスなどのスイッチインターフェイスに対する **show interface** コマンドの各フィールドの説明を示します。**show interface** コマンドでも表示されるフィールドについては、表 7-6 を参照してください。

表 7-6　スイッチ インターフェイスについての show interface の各フィールド

フィールド	説明
switch ingress policy drops	このドロップは通常、ポートが正しく設定されていないときに表示されます。このドロップは、デフォルトまたはユーザ設定のスイッチ ポート設定の結果としてスイッチ ポート内でパケットが正常に転送できない場合に増分されます。このドロップの原因として、次のコンフィギュレーションが考えられます。 • **nameif** コマンドが VLAN インターフェイス上で設定されていない。 (注)　同じ VLAN 内のインターフェイスに、**nameif** コマンドが設定されていなかった場合でも、VLAN 内のスイッチングは正常で、このカウンタは増分されません。 • VLAN がシャットダウンしている。 • アクセス ポートで 802.1Q タグが付いたパケットを受信した。 • トランク ポートで許可されないタグまたはタグのないパケットを受信した。 • ASA が、イーサネット キープアライブを持つ別のシスコ デバイスに接続されている。たとえば、Cisco IOS ソフトウェアではインターフェイス ヘルス状態を確認するためにイーサネット ループバック パケットを使用します。このパケットは、他のデバイスによって受信されるためのものではなく、パケットをただ送信できることによって、ヘルス状態が確認されます。これらのタイプのパケットはスイッチ ポートでドロップされ、カウンタが増分されます。
switch egress policy drops	現在使用されていません。

次に、**show interface detail** コマンドの出力例を示します。次に、すべてのインターフェイス（プラットフォームに存在する場合は内部インターフェイスを含む）についての詳細なインターフェイス統計情報および非対称ルーティング統計情報（**asr-group** コマンドでイネーブルにされている場合）を表示する例を示します。

```
ciscoasa# show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

表 7-7 に、**show interface detail** コマンドの各フィールドの説明を示します。**show interface** コマンドでも表示されるフィールドについては、表 7-7 を参照してください。

表 7-7　show interface detail の各フィールド

フィールド	説明
Demux drops	（内部データ インターフェイスのみ）ASA が SSM インターフェイスからのパケットを逆多重化できなかったためドロップしたパケットの数。SSM インターフェイスはバックプレーンを介してネイティブ インターフェイスと通信し、すべての SSM インターフェイスからのパケットはバックプレーン上で多重化されます。
Control Point Interface States:	

表 7-7　show interface detail の各フィールド(続き)

フィールド	説明
Interface number	デバッグに使用される 0 から始まる番号で、このインターフェイスが作成された順番を示します。
Interface config status	管理ステートは次のとおりです。 • active:インターフェイスはシャット ダウンされていません。 • not active:インターフェイスは **shutdown** コマンドでシャット ダウンされています。
インターフェイスの状態	インターフェイスの実際の状態。この状態は通常、上記の config status と一致します。ハイ アベイラビリティに設定した場合、ASA は必要に応じてインターフェイスを動作状態またはダウン状態にするため、不一致が生じる可能性があります。
Asymmetrical Routing Statistics:	
Received X1 packets	このインターフェイスで受信した ASR パケットの数。
Transmitted X2 packets	このインターフェイスで送信した ASR パケットの数。
Dropped X3 packets	このインターフェイスでドロップした ASR パケットの数。パケットは、パケットを転送しようとしたときにインターフェイスがダウン状態の場合にドロップされることがあります。

次に、ASA 5512-X ～ ASA 5555-X 上の **show interface detail** コマンドの出力例を示します。この例では、ASA とソフトウェア モジュールの両方の管理 0/0 インターフェイス(「Internal-Data0/1」として表示)の統計情報を組み合わせて示しています。出力には、Internal-Control0/0 インターフェイスも示されています。これは、ソフトウェア モジュールと ASA 間の制御トラフィックに使用されています。

```
Interface Internal-Data0/1 "ipsmgmt", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "ipsmgmt":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
```

```
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active

Interface Internal-Control0/0 "cplane", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "cplane":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
```

show interface vni 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

show interface vni 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
delay	インターフェイスの遅延メトリックを変更します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show interface ip brief

インターフェイスの IP アドレスおよびステータスを表示するには、特権 EXEC モードで **show interface ip brief** コマンドを使用します。

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] **ip brief**

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
サブインターフェイス	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

インターフェイスを指定しない場合、ASA はすべてのインターフェイスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント[1]	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	トランスペアレント モードでの VLAN インターフェイスおよび管理 0/0 インターフェイスまたはサブインターフェイスのサポートが追加されました。
9.10(1)	Firepower 2100/4100/9300 デバイスのスーパバイザ アソシエーションのサポートが追加されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名またはインターフェイス名はコンテキスト内だけで指定できます。

出力表示の詳細については、「例」を参照してください。

例

次に、**show ip brief** コマンドの出力例を示します。

```
ciscoasa# show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   admin  down            down
    GigabitEthernet0/2         10.1.1.50       YES manual  admin down            down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    admin down            down
    Management0/0              209.165.201.3   YES CONFIG  up
```

次に、FXOS が搭載された ASA での **show ip brief** コマンドの出力例を示します。

```
ciscoasa# sh int ip br
    Interface                  IP-Address      OK?           Method Status      Protocol
    Internal-Data0/0           unassigned      YES           unset  up          up
    Vlan10                     172.18.249.190  YES           CONFIG up          up
    Vlan80                     80.1.1.1        YES           manual up          up
    Vlan300                    14.30.1.1       YES           CONFIG up          up
    ....
    Ethernet1/1                unassigned      YES           unset  up          up
    Ethernet1/2                unassigned      YES           unset  down        down
    Ethernet1/3                unassigned      unassociated  unset  admin down  down
    Ethernet1/4                unassigned      unassociated  unset  admin down  down
    Ethernet1/5                unassigned      YES           unset  up          up
    Ethernet1/6                unassigned      unassociated  unset  down        down
    Ethernet1/7                unassigned      unassociated  unset  down        down
    Ethernet1/8                unassigned      unassociated  unset  up          up
    Internal-Data1/1           169.254.1.1     YES           unset  up          up
    Management1/1              unassigned      YES           unset  up          up
    BVI50                      50.1.1.3        YES           CONFIG up          up
    Port-channel3              unassigned      YES           unset  down        down
    Port-channel8              8.0.0.1         YES           manual up          up
```

表 7-7 に、各フィールドの説明を示します。

表 7-8　show interface ip brief の各フィールド

フィールド	説明
Interface	**allocate-interface** コマンドを使用して設定した場合の、マルチ コンテキスト モードでのインターフェイス ID またはマッピング名。すべてのインターフェイスを表示すると、AIP SSM の内部インターフェイスが ASA にインストールされている場合は、それらのインターフェイスに関する情報が表示されます。内部インターフェイスは、ユーザによる設定は不可能です。情報はデバッグだけを目的としています。
IP-Address	インターフェイスの IP アドレス。

表 7-8　show interface ip brief の各フィールド(続き)

フィールド	説明
OK?	インターフェイスがスーパーバイザに関連付けられていない場合、この列には「unassociated」と表示されます。インターフェイスがスーパーバイザに関連付けられている場合は「YES」と表示されます。この状態は、Firepower 2100/4100/9300 インターフェイスとデバイスにのみ適用されます。 FXOS ベースの ASA デバイスの場合は、インターフェイスがポートチャネルに追加されるとこの列に「unassociated」と表示されます。 その他のデバイスでは、この列は現在使用されておらず、常に「Yes」と表示されます。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 • unset：IP アドレスは設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。
Status	管理ステートは次のとおりです。 • up：インターフェイスはシャットダウンされません。 • admin down：インターフェイスは、**shutdown** コマンドを使用してシャットダウンされます。
Protocol	回線ステータスは次のとおりです。 • up：動作するケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address	インターフェイスの IP アドレス、またはトランスペアレント ファイアウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show inventory

製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）が割り当てられているネットワーク デバイスにインストールされているすべてのシスコ製品に関する情報を表示するには、ユーザ EXEC モードで **show inventory** コマンドを使用します。

show inventory [*mod_id*]

構文の説明

mod_id	（オプション）モジュール ID またはスロット番号（0 ～ 3）を指定します。

デフォルト

項目のインベントリを表示するスロットを指定しない場合は、すべてのモジュール（電源モジュールを含む）のインベントリ情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.4(2)	SSP の出力が追加されました。さらに、デュアル SSP インストールのサポートが追加されました。
8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X および 5555-X（シャーシ、冗長電源、I/O 拡張カード）の出力が追加されました。
9.1(1)	ASA CX モジュールの出力が追加されました。

使用上のガイドライン

show inventory コマンドは、各シスコ製品についてのインベントリ情報を UDI 形式で取得および表示します。UDI 形式とは、製品 ID（PID）、バージョン番号（VID）、およびシリアル番号（SN）という 3 つの別個のデータ要素の組み合わせです。

PID は製品を発注するための名前で、従来は「製品名」または「部品番号」と呼ばれていました。これは、正しい交換部品を発注するために使用する ID です。

VID は製品のバージョンです。製品が変更されると、VID は、製品の変更通知を管理する業界ガイドラインである Telcordia GR-209-CORE から定めた厳格なプロセスに従って増分されます。

SN はベンダー固有の製品の通し番号です。それぞれの製品には工場で割り当てた独自のシリアル番号があり、現場では変更できません。シリアル番号は、製品の個々の固有のインスタンスを識別するための手段です。シリアル番号は、デバイスのさまざまなコンポーネントに応じてその長さが異なる場合があります。

UDI では各製品をエンティティと呼びます。シャーシなどの一部のエンティティには、スロットのようなサブエンティティがあります。各エンティティは、シスコ エンティティごとに階層的に配置された論理的な表示順で別々の行に表示されます。

オプションを指定せずに **show inventory** コマンドを使用すると、ネットワーキング デバイスに取り付けられており、PID が割り当てられているシスコ エンティティのリストが表示されます。

シスコ エンティティに PID が割り当てられていない場合、そのエンティティは取得または表示されません。

(注) 2 つの SSP が同じシャーシに取り付けられている場合は、モジュールの番号がシャーシ内でのモジュールの物理的な場所を示します。スロット 0 に取り付けられた SSP が、常にシャーシ マスターとなります。センサーは、SSP が関連付けられている場合にのみ、出力に表示されます。

出力内の用語 *module* は、物理スロットと同等です。SSP 自体の説明においては、物理スロット 0 に取り付けられている場合には出力に module: 0、それ以外の場合は module: 1 が含まれます。ターゲット SSP がシャーシ マスターである場合、**show inventory** コマンドの出力には電源や冷却ファンが含まれます。それ以外の場合、これらのコンポーネントは省略されます。

ASA 5500-X シリーズのハードウェア上の制限により、シリアル番号が表示されない場合があります。これらのモデルの PCI-E I/O（NIC）オプション カードの UDI 表示では、カード タイプは 2 つのみですが、出力はシャーシ タイプに応じて 6 通りになります。これは、指定されたシャーシに応じて異なる PCI-E ブラケット アセンブリが使用されるためです。次に、各 PCI-E I/O カード アセンブリについて予想される出力を示します。たとえば、Silicom SFP NIC カードが検出された場合、UDI 表示はこのカードが取り付けられているデバイスによって決定されます。VID および S/N の値は N/A です。これは、これらの値が電子的に格納されていないためです。

ASA 5512-X または 5515-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

ASA 5525-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

ASA 5545-X または 5555-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

ASA 5512-X または 5515-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

ASA 5525-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

ASA 5545-X または 5555-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

例

次に、キーワードや引数を指定していない **show inventory** コマンドの出力例を示します。この出力例は、ASA に取り付けられている、PID が割り当てられている各シスコ エンティティのリストを示しています（ASA CX モジュール用に使用されているストレージ デバイスを含む）。

```
ciscoasa> show inventory
Name: "Chassis", DESCR: "ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5555            , VID: V01     , SN: FGL170441BU

Name: "power supply 1", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC         , VID: N/A     , SN: 2CS1AX

Name: "Storage Device 1", DESCR: "Micron 128 GB SSD MLC, Model Number: C400-MTFDDAC128MAM"
PID: N/A                , VID: N/A     , SN: MXA174201RR
```

次に、デュアル SSP インストールのシャーシ マスター上の **show inventory** コマンドの出力例を示します。

```
ciscoasa> show inventory
Name: "module 0", DESCR: "ASA 5585-X Security Services Processor-40 w 6GE,4 SFP+"
PID: ASA5585-SSP-40     , VID: V01     , SN: JAF1436ACLJ

Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585            , VID: V01     , SN: 123456789AB

Name: "fan", DESCR: "ASA 5585-X Fan Module"
PID: ASA5585-FAN        , VID: V01     , SN: POG1434000G

Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC     , VID: V01     , SN: POG1434002K
```

このコマンドは取り外し可能なモジュールのみを表示します。したがって、ASA で **show interface brief** を実行すると、EPM のすべての SFP インターフェイスが表示されますが、ASA で **show inventory** コマンドを実行すると、SFP が接続されているインターフェイスのデータのみが表示されます。次に、接続されている SFP インターフェイスでの **show inventory**コマンドの出力例を示します。

```
ciscoasa> show inventory
Name: "Ethernet 1/13", DESCR: "h10g-acu1m"
PID: SFP-10G-AOC1M, VID: , SN: A4Z1942K0UC-B
```

表 7-9 に、この出力で表示されるフィールドについて説明します。

表 7-9　show inventory のフィールドの説明

フィールド	説明
Name	シスコ エンティティに割り当てられた物理名（テキスト ストリング）。たとえば、コンソール、SSP、または「1」などの簡易コンポーネント番号（ポートまたはモジュールの番号）など、デバイスの物理コンポーネント命名構文に応じて異なります。RFC 2737 の entPhysicalName MIB 変数に相当します。
DESCR	オブジェクトを特徴付けるシスコ エンティティの物理的な説明。RFC 2737 の entPhysicalDesc MIB 変数に相当します。
PID	エンティティ製品 ID。RFC 2737 の entPhysicalModelName MIB 変数に相当します。

表 7-9　show inventory のフィールドの説明（続き）

フィールド	説明
VID	エンティティのバージョン番号。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。
SN	エンティティのシリアル番号。RFC 2737 の entPhysicalSerialNum MIB 変数に相当します。

関連コマンド

コマンド	説明
show diag	ネットワーキング デバイスのコントローラ、インターフェイス プロセッサ、およびポート アダプタについての診断情報を表示します。
show tech-support	ルータが問題を報告したときに、ルータに関する一般情報を表示します。

show ip address

インターフェイス IP アドレス（トランスペアレント モードの場合は管理 IP アドレス）を表示するには、特権 EXEC モードで **show ip address** コマンドを使用します。

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*]

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
サブインターフェイス	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

インターフェイスを指定しない場合、ASA はすべてのインターフェイス IP アドレスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	VLAN インターフェイスのサポートが追加されました。

使用上のガイドライン

このコマンドは、ハイ アベイラビリティを設定するときのためのプライマリ IP アドレス（表示では「System」と記載される）と現在の IP アドレスを表示します。ユニットがアクティブの場合、システム IP アドレスと現在の IP アドレスは一致します。ユニットがスタンバイの場合、現在の IP アドレスにはスタンバイ アドレスが表示されます。

例

次に、**show ip address** コマンドの出力例を示します。

```
ciscoasa# show ip address
System IP Addresses:
Interface                Name          IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt          10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside        10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside       209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz           209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface                Name          IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt          10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside        10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside       209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz           209.165.200.225 255.255.255.224   manual
```

表 7-7 に、各フィールドの説明を示します。

表 7-10　show ip address の各フィールド

フィールド	説明
Interface	**allocate-interface** コマンドを使用して設定した場合の、マルチ コンテキスト モードでのインターフェイス ID またはマッピング名。
名前	**nameif** コマンドで設定されたインターフェイス名。
IP address	インターフェイスの IP アドレス。
サブネット マスク	IP アドレスのサブネット マスク。
方式	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 • unset：IP アドレスは設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show ip address dhcp

インターフェイスに対する DHCP リースまたはサーバに関する詳細情報を表示するには、特権 EXEC モードで **show ip address dhcp** コマンドを使用します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp** {**lease** | **server**}

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp lease** {**proxy** | **server**} {**summary**}

構文の説明

interface_name	**nameif** コマンドを使用して設定されたインターフェイス名を指定します。
lease	DHCP リースに関する情報を表示します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
proxy	IPL テーブル内のプロキシ エントリを表示します。
サーバ	IPL テーブル内のサーバ エントリを表示します。
サブインターフェイス	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
summary	エントリの要約を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント[1]	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.0(1)	新しいサーバ機能に適応するための **lease** キーワードおよび **server** キーワードが追加されました。
7.2(1)	トランスペアレント モードでの VLAN インターフェイスおよび管理 0/0 インターフェイスまたはサブインターフェイスのサポートが追加されました。
9.1(4)	新しいサーバ機能に適応するための **proxy** キーワードおよび **summary** キーワードが追加されました。

使用上のガイドライン

出力の説明については、「例」を参照してください。

例

次に、**show ip address dhcp lease** コマンドの出力例を示します。

```
ciscoasa# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

表 7-7 に、各フィールドの説明を示します。

表 7-11　show ip address dhcp lease の各フィールド

フィールド	説明
Temp IP Addr	インターフェイスに割り当てられている IP アドレス。
Temp sub net mask	インターフェイスに割り当てられているサブネット マスク。
DHCP Lease server	DHCP サーバ アドレス。

表 7-11　show ip address dhcp lease の各フィールド(続き)

フィールド	説明
state	DHCP リースの状態で、次のとおりです。 • [Initial]:初期化状態で、ASA がリースを取得するプロセスを開始します。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。 • [Selecting]:ASA は 1 つ以上の DHCP サーバから DHCPOFFER メッセージを受信することを待機しており、メッセージを選択できます。 • [Requesting]:ASA は、要求を送信した送信先サーバからの応答を待機しています。 • Purging:クライアントが IP アドレスを解放したか、他のエラーが発生したため、ASA はリースを削除します。 • [Bound]:ASA は有効なリースを保持し、正常に動作しています。 • [Renewing]:ASA はリースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信し、応答を待機します。 • [Rebinding]:ASA は元のサーバのリースを更新することに失敗したため、いずれかのサーバから応答を受け取るかリースが終了するまで DHCPREQUEST メッセージを送信します。 • [Holddown]:ASA はリースを削除するプロセスを開始しました。 • [Releasing]:ASA は IP アドレスが不要になったことを示すリリース メッセージをサーバに送信します。
DHCP transaction id	クライアントによって選択され、要求メッセージを関連付けるためにクライアントとサーバによって使用される乱数。
Lease	DHCP サーバによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。
Renewal	インターフェイスがこのリースを自動的に更新しようとするまでの時間の長さ。
Rebind	ASA が DHCP サーバに再バインドしようとするまでの時間の長さ。再バインドが発生するのは、ASA が元の DHCP サーバと通信できず、リース期間の 87.5% を経過した場合です。ASA は、DHCP 要求をブロードキャストすることによって、使用可能な任意の DHCP サーバに接続を試みます。
Temp default-gateway addr	DHCP サーバによって指定されるデフォルト ゲートウェイ アドレス。
Temp ip static route0	デフォルト スタティック ルート。
Next timer fires after	内部タイマーがトリガーするまでの秒数。
リトライ回数	ASA がリースを設定しようとしているとき、このフィールドは、ASA が DHCP メッセージの送信を試行した回数を示します。たとえば、ASA が Selecting 状態の場合、この値は ASA が探索メッセージを送信した回数を示します。ASA が Requesting 状態の場合、この値は ASA が要求メッセージを送信した回数を示します。
Client-ID	サーバとのすべての通信に使用したクライアント ID。

表 7-11　show ip address dhcp lease の各フィールド(続き)

フィールド	説明
Proxy	このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。
Proxy Network	要求されたネットワーク。
Hostname	クライアントのホスト名。

次に、**show ip address dhcp server** コマンドの出力例を示します。

```
ciscoasa# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

表 7-12 に、各フィールドの説明を示します。

表 7-12　show ip address dhcp server の各フィールド

フィールド	説明
DHCP サーバ	このインターフェイスがリースを取得した DHCP サーバ アドレス。最上位エントリ(「ANY」)はデフォルト サーバで常に存在します。
Leases	サーバから取得したリースの数。インターフェイスの場合、リースの数は一般的に 1 です。VPN 用のプロキシを実行中のインターフェイスに対してサーバがアドレスを提供している場合、リースは複数となります。
Offers	サーバからのオファーの数。
Requests	サーバに送信された要求の数。
Acks	サーバから受信した確認応答の数。
Naks	サーバから受信した否定応答の数。
Declines	サーバから受信した拒否の数。
リリース	サーバに送信されたリリースの数。
Bad	サーバから受信した不良パケットの数。
DNS0	DHCP サーバから取得したプライマリ DNS サーバ アドレス。
DNS1	DHCP サーバから取得したセカンダリ DNS サーバ アドレス。
WINS0	DHCP サーバから取得したプライマリ WINS サーバ アドレス。
WINS1	DHCP サーバから取得したセカンダリ WINS サーバ アドレス。
Subnet	DHCP サーバから取得したサブネット アドレス。
DNS ドメイン	DHCP サーバから取得したドメイン。

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address dhcp	インターフェイスで DHCP サーバから IP アドレスを取得できるように設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip address pppoe

PPPoE 接続に関する詳細情報を表示するには、特権 EXEC モードで **show ip address pppoe** コマンドを使用します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*} **pppoe**

構文の説明

interface_name	**nameif** コマンドを使用して設定されたインターフェイス名を指定します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
サブインターフェイス	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント[1]	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

出力の説明については、「例」を参照してください。

例

次に、**show ip address pppoe** コマンドの出力例を示します。

```
ciscoasa# show ip address outside pppoe
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address ppoe	PPPoE サーバから IP アドレスを取得するようにインターフェイスを設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip audit count

監査ポリシーをインターフェイスに適用するときシグニチャの一致数を表示するには、特権 EXEC モードで **show ip audit count** コマンドを使用します。

show ip audit count [**global** | **interface** *interface_name*]

構文の説明

global	(デフォルト)すべてのインターフェイスについての一致数を表示します。
interface *interface_name*	(任意)指定したインターフェイスについての一致数を表示します。

デフォルト

キーワードを指定しない場合、このコマンドは、すべてのインターフェイスについての一致数を表示します(**global**)。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

監査ポリシーを作成するには、**ip audit name** コマンドを使用します。ポリシーを適用するには、**ip audit interface** コマンドを使用します。

例

次に、**show ip audit count** コマンドの出力例を示します。

```
ciscoasa# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
```

```
1103 A IP Teardrop                 0
2000 I ICMP Echo Reply             0
2001 I ICMP Unreachable            0
2002 I ICMP Source Quench          0
2003 I ICMP Redirect               0
2004 I ICMP Echo Request           10
2005 I ICMP Time Exceed            0
2006 I ICMP Parameter Problem      0
2007 I ICMP Time Request           0
2008 I ICMP Time Reply             0
2009 I ICMP Info Request           0
2010 I ICMP Info Reply             0
2011 I ICMP Address Mask Request   0
2012 I ICMP Address Mask Reply     0
2150 A Fragmented ICMP             0
2151 A Large ICMP                  0
2154 A Ping of Death               0
3040 A TCP No Flags                0
3041 A TCP SYN & FIN Flags Only    0
3042 A TCP FIN Flag Only           0
3153 A FTP Improper Address        0
3154 A FTP Improper Port           0
4050 A Bomb                        0
4051 A Snork                       0
4052 A Chargen                     0
6050 I DNS Host Info               0
6051 I DNS Zone Xfer               0
6052 I DNS Zone Xfer High Port     0
6053 I DNS All Records             0
6100 I RPC Port Registration       0
6101 I RPC Port Unregistration     0
6102 I RPC Dump                    0
6103 A Proxied RPC                 0
6150 I ypserv Portmap Request      0
6151 I ypbind Portmap Request      0
6152 I yppasswdd Portmap Request   0
6153 I ypupdated Portmap Request   0
6154 I ypxfrd Portmap Request      0
6155 I mountd Portmap Request      0
6175 I rexd Portmap Request        0
6180 I rexd Attempt                0
6190 A statd Buffer Overflow       0

IP AUDIT INTERFACE COUNTERS: inside
...
```

関連コマンド

コマンド	説明
clear ip audit count	監査ポリシーのシグニチャ一致カウントをクリアします。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

show ip local pool

IPv4 アドレス プール情報を表示するには、特権 EXEC モードで **show ip local pool** コマンドを使用します。

show ip local pool interface *pool_name*

構文の説明

pool_name	アドレス プールの名前。プールのリストを確認するには、? を入力します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用し、**ip local pool** コマンドで作成した IPv4 アドレス プールの内容を表示します。これらのプールは、リモート アクセス VPN およびクラスタリングで使用されます。IPv6 アドレス プールを表示するには、**ipv6 local pool** コマンドを使用します。

例

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。

```
ciscoasa# show ip local pool test-ipv4-pool
Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0

Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
... (remaining output redacted)...
```

関連コマンド

コマンド	説明
ip local pool	IPv4 アドレス プールを設定します。

show ip verify statistics

ユニキャスト RPF 機能が原因でドロップしたパケットの数を表示するには、特権 EXEC モードで **show ip verify statistics** コマンドを使用します。ユニキャスト RPF をイネーブルにするには、**ip verify reverse-path** コマンドを使用します。

show ip verify statistics [interface *interface_name*]

構文の説明

interface *interface_name*	（任意）指定したインターフェイスの統計情報を表示します。

デフォルト

このコマンドは、すべてのインターフェイスの統計情報を表示します。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show ip verify statistics** コマンドの出力例を示します。

```
ciscoasa# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
ip verify reverse-path	IP スプーフィングを防ぐユニキャスト リバース パス転送機能をイネーブルにします。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

show ips

AIP SSM で設定されている使用可能な IPS 仮想センサーをすべて表示するには、特権 EXEC モードで **show ips** コマンドを使用します。

show ips [**detail**]

構文の説明

detail	（任意）センサーの ID 番号と名前を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、このコマンドは、システム実行スペースで入力するとすべての仮想センサーを表示しますが、コンテキスト実行スペース内ではコンテキストに割り当てられた仮想センサーのみ表示します。仮想センサーをコンテキストに割り当てることについては、**allocate-ips** コマンドを参照してください。

仮想センサーは IPS バージョン 6.0 以降で使用できます。

例

次に、**show ips** コマンドの出力例を示します。

```
ciscoasa# show ips
Sensor name
------------
ips1
ips2
```

次に、**show ips detail** コマンドの出力例を示します。

```
ciscoasa# show ips detail
Sensor name              Sensor ID
------------             ---------
ips1                     1
ips2                     2
```

関連コマンド

コマンド	説明
allocate-ips	セキュリティ コンテキストに仮想センサーを割り当てます。
ips	トラフィックを AIP SSM に迂回させます。

show ipsec df-bit

指定されたインターフェイスの IPsec パケットの IPsec do-not-fragment（DF ビット）ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec df-bit** コマンドを使用します。また、同じ意味を持つ **show crypto ipsec df-bit** コマンドも使用できます。

show ipsec df-bit *interface*

構文の説明

interface	インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

df ビットの設定によって、カプセル化されたヘッダーの do-not-fragment（DF）ビットのシステムによる処理方法が決まります。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。この設定に基づき、システムは暗号の適用時に外側の IPsec ヘッダーに対するクリアテキスト パケットの DF ビットの設定をクリアするか、設定するか、コピーするかのいずれかを実行します。

例

次に、inside というインターフェイスの IPsec DF ビット ポリシーを表示する例を示します。

```
ciscoasa(config)# show ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPsec パケットの IPsec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPsec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec fragmentation** コマンドを使用します。また、同じ意味を持つ **show crypto ipsec fragmentation** コマンドも使用できます。

show ipsec fragmentation *interface*

構文の説明

interface	インターフェイス名を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

VPN に対するパケットを暗号化する際、システムはパケット長をアウトバウンド インターフェイスの MTU と比較します。パケットの暗号化が MTU を超える場合は、パケットをフラグメント化する必要があります。このコマンドは、パケットを暗号化した後（after-encryption）、または暗号化する前（before-encryption）にシステムがパケットをフラグメント化するかどうかを表示します。暗号化前のパケットのフラグメント化は、事前フラグメント化とも呼ばれ、暗号化パフォーマンス全体を向上させるため、システムのデフォルト動作になっています。

例

次に、グローバル コンフィギュレーション モードで、inside という名前のインターフェイスの IPsec フラグメンテーション ポリシーを表示する例を示します。

```
ciscoasa(config)# show ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPsec パケットの DF ビット ポリシーを設定します。
show ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show ipsec policy

OSPFv3 に設定されている IPsec セキュア ソケット API（SS API）セキュリティ ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec policy** コマンドを使用します。また、このコマンドの別の形式である **show crypto ipsec policy** を使用することもできます。

show ipsec policy

構文の説明

このコマンドには、キーワードや変数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、OSPFv3 認証と暗号方式ポリシーを表示する例を示します。

```
ciscoasa# show ipsec policy

Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901
Outbound ESP Auth Key:   12345678901234567890123456789012345678901
Inbound  ESP Cipher Key: 1234567890123456789012345678901
Outbound ESP Cipher Key: 1234567890123456789012345678901
Transform set:    esp-aes esp-sha-hmac
```

関連コマンド

コマンド	説明
ipv6 ospf encryption	OSPFv3 の認証と暗号方式ポリシーを設定します。
show crypto sockets	セキュアなソケット情報を表示します。
show ipv6 ospf interface	OSPFv3 インターフェイスに関する情報を表示します。

show ipsec sa

IPsec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa** コマンドを使用します。また、このコマンドの代替形式の **show crypto ipsec sa** も使用できます。

show ipsec sa [**assigned-address** *hostname or IP address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

構文の説明

assigned-address	(オプション)指定されたホスト名または IP アドレスの IPsec SA を表示します。
detail	(任意)表示されているものに対する詳細なエラー情報を表示します。
entry	(オプション)IPsec SA をピア アドレスの順に表示します。
identity	(オプション)IPsec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
inactive	(オプション)トラフィックを渡すことができない IPsec SA を表示します。
map *map-name*	(オプション)指定されたクリプト マップの IPsec SA を表示します。
peer *peer-addr*	(オプション)指定されたピア IP アドレスの IPsec SA を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	OSPFv3 およびマルチ コンテキスト モードのサポートが追加されました。
9.1(4)	割り当てられた IPv6 アドレスを反映し、IKEv2 デュアルトラフィックの実行時に、GRE トランスポート モードのセキュリティ アソシエーションを示すように、出力が更新されました。

例

次に、グローバル コンフィギュレーション モードで、IPsec SA を表示する例を示します。ここには、割り当てられた IPv6 アドレス、およびトランスポート モードと GRE カプセル化の表示が含まれます。

```
ciscoasa(config)# sho ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 4

     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

次に、グローバル コンフィギュレーション モードで、IPsec SA を表示する例を示します。ここには使用中の設定が含まれ、トンネルが OSPFv3 として示されています。

```
ciscoasa(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5
```

```
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

(注) IPSec SA ポリシーに、フラグメンテーションは IPsec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーに、フラグメンテーションは IPsec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次に、グローバル コンフィギュレーション モードで、def という名前のクリプト マップの IPsec SA を表示する例を示します。

```
ciscoasa(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
```

```
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry** に対する IPsec SA を表示する例を示します。

```
ciscoasa(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
```

```
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry detail** を使用して IPsec SA を表示する例を示します。

```
ciscoasa(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
```

```
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

次に、キーワード **identity** を使用した IPsec SA の例を示します。

```
ciscoasa(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
```

```
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次に、キーワード **identity** および **detail** を使用した IPsec SA の例を示します。

```
ciscoasa(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次の例では、IPv6 で割り当てられたアドレスに基づいて IPSec SA を表示しています。

```
ciscoasa(config)# sho ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
```

```
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0      #TFC
rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35

      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show ipsec sa summary

IPsec SA の要約を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa summary** コマンドを使用します。

show ipsec sa summary

構文の説明

このコマンドには、引数または変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、グローバル コンフィギュレーション モードで、次の接続タイプ別に IPsec SA の要約を表示する例を示します。

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN ロード バランシング

```
ciscoasa(config)# show ipsec sa summary

Current IPsec SA's:           Peak IPsec SA's:
IPsec            :     2        Peak Concurrent SA  :    14
IPsec over UDP   :     2        Peak Concurrent L2L :     0
IPsec over NAT-T :     4        Peak Concurrent RA  :    14
IPsec over TCP   :     6
IPsec VPN LB     :     0
Total            :    14
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPsec SA を完全に削除するか、特定のパラメータに基づいて削除します。
show ipsec sa	IPsec SA のリストを表示します。
show ipsec stats	IPsec 統計情報のリストを表示します。

show ipsec stats

IPSec 統計情報のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec stats** コマンドを使用します。

show ipsec stats

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ESPv3 統計情報が IPSec サブシステムとともに示され、マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

次に、出力エントリが示す内容について説明した表を示します。

出力	説明
IPsec Global Statistics	このセクションは、ASA がサポートする IPsec トンネルの総数に関係します。
Active tunnels	現在接続されている IPsec トンネルの数。
Previous tunnels	接続されたことがある IPsec トンネルの数(アクティブなトンネルを含む)。
着信	このセクションは、IPsec トンネルを介して受信した着信暗号トラフィックに関係します。
Bytes	受信した暗号トラフィックのバイト数。

出力(続き)	説明 (続き)
Decompressed bytes	圧縮解除が実行された後に受信された暗号トラフィックのバイト数(該当する場合)。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。
Packets	受信された IPsec 暗号化パケットの数。
Dropped packets	受信されたがエラーのためドロップされた IPsec 暗号化パケットの数。
Replay failures	受信された IPsec 暗号化パケットについて検出されたアンチリプレイの失敗数。
Authentications	受信された IPsec 暗号化パケットについて実行された認証の成功数。
Authentication failures	受信された IPsec 暗号化パケットについて検出された認証の失敗数。
Decryptions	受信された IPsec 暗号化パケットについて実行された復号化の成功数。
Decryption failures	受信された IPsec 暗号化パケットについて検出された復号の失敗数。
Decapsulated fragments needing reassembly	再構築が必要な IP フラグメントを含む復号 IPSec パケットの数。
発信	このセクションは、IPsec トラフィックを介して送信される発信クリアテキスト トラフィックに関係します。
Bytes	IPsec トンネルを介して暗号化および送信されるクリアテキスト トラフィックのバイト数。
Uncompressed bytes	IPsec トンネルを介して暗号化および送信される圧縮解除されたクリアテキスト トラフィックのバイト数。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。
Packets	IPsec トンネルを介して暗号化および送信されるクリアテキスト パケットの数。
Dropped packets	IPsec トンネルを介して暗号化および送信されるが、エラーが原因でドロップされたクリアテキスト パケットの数。
Authentications	IPsec トンネルを介して送信されるパケットについて実行された認証の成功数。
Authentication failures	IPsec トンネルを介して送信されるパケットについて検出された認証の失敗数。
Encryptions	IPsec トンネルを介して送信されるパケットについて実行された暗号化の成功数。
Encryption failures	IPsec トンネルを介して送信されるパケットについて検出された暗号化の失敗数。
Fragmentation successes	発信 IPsec パケットの変換の一部として実行されたフラグメンテーション操作の成功数。

出力（続き）	説明（続き）
Pre-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。
Post-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragmentation failures	発信 IPsec パケットの変換中に発生したフラグメンテーションの失敗数。
Pre-fragmentation failures	発信 IPsec パケットの変換中に発生したプリフラグメンテーションの失敗数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。
Post-fragmentation failure	発信 IPsec パケットの変換中に発生したポストフラグメンテーションの失敗数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragments created	IPsec の変換の一部として作成されたフラグメントの数。
PMTUs sent	IPsec システムによって送信されたパス MTU メッセージの数。IPsec は、暗号化後に、IPsec トンネルを介して送信するには大きすぎるパケットを送信している内部ホストに対して PMTU メッセージを送信します。PMTU メッセージは、ホストの MTU を低くして、IPsec トンネルを介して送信するパケットのサイズを小さくすることをホストに求めるメッセージです。
PMTUs recvd	IPsec システムによって受信されたパス MTU メッセージの数。IPsec は、トンネルを介して送信するパケットが大きすぎてネットワーク要素を通過できない場合、ダウンストリームのネットワーク要素からパス MTU メッセージを受信します。パス MTU メッセージを受信すると、IPsec は通常、トンネル MTU を低くします。
Protocol failures	受信した不正な形式の IPsec パケットの数。
Missing SA failures	指定された IPsec セキュリティ アソシエーションが存在しない、要求された IPsec の動作の数。
System capacity failures	IPsec システムの容量が十分でないためデータ レートをサポートできないことが原因で完了できない IPsec の動作の数。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
ciscoasa(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	指定されたパラメータに基づいて、IPsec SA またはカウンタをクリアします。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定されたパラメータに基づいて IPsec SA を表示します。
show ipsec sa summary	IPsec SA の要約を表示します。

show ipv6 access-list コマンド～ show ipv6 traffic コマンド

show ipv6 access-list

IPv6 アクセス リストを表示するには、特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。IPv6 アクセス リストは、ASA を通過できる IPv6 トラフィックを決定します。

show ipv6 access-list [*id* [*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*]]

構文の説明

任意	（任意）IPv6 プレフィックス ::/0 の省略形。
host *source-ipv6-address*	（任意）特定のホストの IPv6 アドレス。指定した場合、指定されたホストについてのアクセス ルールのみが表示されます。
id	（任意）アクセス リストの名前。指定した場合、指定されたアクセス リストのみが表示されます。
source-ipv6-prefix /prefix-length	（任意）IPv6 ネットワーク アドレスおよびプレフィックス。指定した場合、指定された IPv6 ネットワークについてのアクセス ルールのみが表示されます。

デフォルト

すべての IPv6 アクセス リストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	IPv6 アクセス ルールが **access-list** コマンドに組み込まれたため、このコマンドの意味がなくなりました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 access-list** コマンドの出力は **show ip access-list** コマンドと類似しています。

このコマンドは、**ipv6 access-list** コマンドを使用して設定したアクセス リストのみを表示します。ASA 9.0(1) では、IPv6 アクセス制御が IPv4 と同じ**アクセス リスト**構造に統合されています。したがって、9.0(1) で始まるソフトウェア バージョンを実行しているシステムでは、**show ipv6 access-list** コマンドの意味がなくなりました。

例

次に、**show ipv6 access-list** コマンドの出力例を示します。inbound、tcptraffic、および outbound という名前の IPv6 アクセス リストが表示されています。

```
ciscoasa# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを作成します。

show ipv6 dhcp

DHCPv6 情報を表示するには、特権 EXEC モードで **show ipv6 dhcp** コマンドを使用します。

show ipv6 dhcp [**client** [**pd**] **statistics** | **interface** [*interface_name* [**statistics**]] | **ha statistics** | **server statistics** | **pool** [*pool_name*]]

構文の説明

クライアント	DHCPv6 クライアント統計情報を表示し、送受信されたメッセージ数の出力を表示します。
pd	DHCPv6 プレフィックス委任クライアントの統計情報を表示します。
statistics	統計情報を表示します。
interface	すべてのインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレス サーバ構成用に設定されている場合（**ipv6 dhcp server** を参照）、このコマンドはサーバによって使用されている DHCPv6 プールをリストします。インターフェイスに DHCPv6 アドレス クライアントまたはプレフィックス委任クライアントの設定がある場合、このコマンドは各クライアントの状態とサーバから受信した値を表示します。
interface_name	（オプション）特定のインターフェイスについて、DHCP サーバまたはクライアントのメッセージの統計情報を表示できます。
ha	DUID 情報がフェールオーバー ユニット間で同期された回数を含め、フェールオーバー ユニット間のトランザクションの統計情報を表示します。
サーバ	DHCPv6 ステートレス サーバの統計情報を表示します。
プール	DHCPv6 プールを表示します。
pool_name	（オプション）指定されたプールを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

引数を指定しない場合、このコマンドは、DHCPv6 クライアントまたはサーバによって使用されているデバイス DUID を表示します。

例

次に、**show ipv6 dhcp** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00030001377E8FD91020
```

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp pool
DHCPv6 pool: Sample-Pool
  Imported DNS server: 2004:abcd:abcd:abcd::2
  Imported DNS server: 2004:abcd:abcd:abcd::4
  Imported Domain name: relay.com
  Imported Domain name: server.com
  SIP server address: 2001::abcd:1
  SIP server domain name: sip.xyz.com
```

次に、**show ipv6 dhcp interface** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
```

```
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0
```

次に、**show ipv6 dhcp interface outside** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp interface outside
GigabitEthernet1/2 is in client mode


 Prefix State is OPEN
 Renew will be sent in 00:02:05
 Address State is OPEN
 Renew for address will be sent in 00:02:06
 List of known servers:
   Reachable via address: fe80::20c:29ff:fe96:1bf4
   DUID: 000100011D9D1712005056A07E06
   Preference: 0
   Configuration parameters:
     IA PD: IA ID 0x00030001, T1 250, T2 400
       Prefix: 2005:abcd:ab03::/48
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     IA NA: IA ID 0x00030001, T1 250, T2 400
       Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     DNS server: 2004:abcd:abcd:abcd::2
     DNS server: 2004:abcd:abcd:abcd::4
     Domain name: relay.com
     Domain name: server.com
     Information refresh time: 0
 Prefix name: Sample-PD
```

次に、**show ipv6 dhcp interface outside statistics** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp interface outside statistics
DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
```

```
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

次に、**show ipv6 dhcp client statistics** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0
```

次に、**show ipv6 dhcp client pd statistics** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                 1
 Total number of Message Validation errors in received messages: 0
```

次に、**show ipv6 dhcp server statistics** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:            0
  Total number of Advertise messages sent:              0
  Total number of Request messages received:            0
  Total number of Renew messages received:              0
```

```
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

次に、**show ipv6 dhcp ha statistics** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

次に、スタンバイ ユニットでの **show ipv6 dhcp ha statistics** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。

コマンド	説明
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

show ipv6 dhcprelay binding

リレー エージェントによって作成されたリレー バインディング エントリを表示するには、特権 EXEC モードで **show ipv6 dhcprelay binding** コマンドを使用します。

show ipv6 dhcprelay binding

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show ipv6 dhcprelay binding コマンドを使用すると、リレー エージェントが作成したリレー バインディング エントリを確認できます。

例

次に、**show ipv6 dhcprelay binding** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcprelay binding
1 in use, 2 most used

Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
60 seconds.

There will be limit of 1000 bindings for each context.
```

関連コマンド

コマンド	説明
show ipv6 dhcprelay statistics	IPv6 DHCP リレー エージェントの情報を表示します。

show ipv6 dhcprelay statistics

IPv6 DHCP リレー エージェント統計情報を表示するには、特権 EXEC モードで **show ipv6 dhcprelay statistics** コマンドを使用します。

show ipv6 dhcprelay statistics

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show ipv6 dhcprelay statistics コマンドを使用すると、IPv6 DHCP リレー エージェント情報を表示できます。

例

次に、**show ipv6 dhcprelay statistics** コマンドの出力例を示します。

```
ciscoasa# show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                    1
  ADVERTISE                                  2
  REQUEST                                    1
  CONFIRM                                    1
  RENEW                                    496
  REBIND                                     0
  REPLY                                    498
  RELEASE                                    0
  DECLINE                                    0
  RECONFIGURE                                0
  INFORMATION-REQUEST                        0
  RELAY-FORWARD                            499
  RELAY-REPLY                              500
```

```
Relay Errors:
  Malformed message:                          0
  Block allocation/duplication failures:      0
  Hop count limit exceeded:                   0
  Forward binding creation failures:          0
  Reply binding lookup failures:              0
  No output route:                            0
  Conflict relay server route:                0
  Failed to add server NP rule:               0
  Unit or context is not active:              0

Total Relay Bindings Created:               498
```

関連コマンド

コマンド	説明
show ipv6 dhcprelay binding	リレー エージェントによって作成されたリレー バインディング エントリを表示します。

show ipv6 general-prefix

DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示するには、特権 EXEC モードで **show ipv6 general-prefix** コマンドを使用します。

show ipv6 general-prefix

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

DHCPv6 サーバによって割り当てられるプレフィックスの推奨有効期間を表示するには、**show ipv6 general-prefix** コマンドを使用します。プレフィックス委任を使用する場合は、IPv6 トラフィックの中断を防ぐために、ASA IPv6 ネイバー探索のルータ アドバタイズメント間隔を DHCPv6 サーバによって割り当てられるプレフィックスの推奨有効期間よりもはるかに小さい値に設定する必要があります。たとえば、DHCPv6 サーバがプレフィックス委任の推奨有効期間を 300 秒に設定している場合は、ASA RA の間隔を 150 秒に設定する必要があります。ASA RA の間隔を設定するには、**ipv6 nd ra-interval** コマンドを参照してください。デフォルトは 200 秒です。

例

次に、**show ipv6 general-prefix** コマンドの出力例を示します。このコマンドは、DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスとそのプレフィックスの他のプロセスへの ASA 配布（「コンシューマ リスト」）を表示します。

```
ciscoasa# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List                Usage count
```

```
BGP network command         1
inside (Address command)    1
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

show ipv6 icmp

すべてのインターフェイス上に設定されている ICMPv6 アクセス ルールを表示するには、特権 EXEC モードで **show ipv6 icmp** コマンドを使用します。

show ipv6 icmp

構文の説明

このコマンドには、引数または変数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ICMPv6 のルールは、デバイス インターフェイスへの ICMPv6 トラフィックを制御します。これらは、through-the-box トラフィックを制御しません。これらのルールを使用して、ICMPv6 コマンド（ping など）をインターフェイスに送信できるアドレスや、送信できる ICMPv6 コマンドのタイプを制御します。これらのルールを表示するには、**show ipv6 icmp** コマンドを使用します。

例

次に、**show ipv6 icmp** コマンドの出力例を示します。

```
ciscoasa show ipv6 icmp
ipv6 icmp permit any inside
```

関連コマンド

コマンド	説明
ipv6 icmp	IPv6 ICMP 管理アクセス ルールを設定します。

show ipv6 interface

IPv6 用に設定されたインターフェイスのステータスを表示するには、特権 EXEC モードで **show ipv6 interface** コマンドを使用します。

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

構文の説明

brief	各インターフェイスの IPv6 ステータスおよびコンフィギュレーションの要約を表示します。
if_name	（任意）**nameif** コマンドで指定された内部または外部のインターフェイス名。指定されたインターフェイスのステータスおよびコンフィギュレーションのみが表示されます。
prefix	（任意）ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。プレフィックスは、IPv6 アドレスのネットワーク部分です。

デフォルト

すべての IPv6 インターフェイスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.10(1)	Firepower 2100/4100/9300 の場合、コマンドの出力は、インターフェイスのスーパーバイザの関連付けステータスを表示するために強化されています。
9.10(1)	Firepower 2100/4100/9300 デバイスのスーパバイザ アソシエーションが存在しないことを示すサポートが追加されました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 interface** コマンドの出力は **show interface** コマンドと類似しています。インターフェイスのハードウェアが使用できる場合、インターフェイスは *up* とマークされます。インターフェイスが双方向通信を提供できる場合、回線プロトコルは *up* とマークされます。Firepower 2100/4100/9300 デバイスでは、スーパバイザが IPv6 インターフェイスに関連付けられていないことを示すために、回線プロトコルのステータスに「スーパバイザに関連付けられていません（not associated with Supervisor）」と表示されます。

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

例

次に、**show ipv6 interface** コマンドの出力例を示します。

```
ciscoasa# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up "not associated with Supervisor"
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

次に、**brief** キーワードを入力した **show ipv6 interface** コマンドの出力例を示します。

```
ciscoasa# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

Firepower 2100/4100/9300 デバイスでは、スーパバイザが IPv6 インターフェイスに関連付けられていないことを示すために、回線プロトコルのステータスに「スーパバイザに関連付けられていません（not associated with Supervisor）」と表示されます。次に、**show ipv6 interface** コマンドの出力例を示します。アドレスからプレフィックスを生成したインターフェイスの特性が表示されています。

```
ciscoasa# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 local pool

IPv6 アドレス プール情報を表示するには、特権 EXEC モードで **show ipv6 local pool** コマンドを使用します。

show ipv6 local pool interface *pool_name*

構文の説明

pool_name	アドレス プールの名前。プールのリストを確認するには、? を入力します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用し、**ipv6 local pool** コマンドで作成した IPv6 アドレス プールの内容を表示します。これらのプールは、リモート アクセス VPN およびクラスタリングで使用されます。IPv4 アドレスプールを表示するには、**ip local pool** コマンドを使用します。

例

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。

```
ciscoasa# show ipv6 local pool test-ipv6-pool
IPv6 Pool test-ipv6-pool
Begin Address: 2001:db8::db8:800:200c:417a
End Address: 2001:db8::db8:800:200c:4188
Prefix Length: 64
Pool Size: 15
Number of used addresses: 0
Number of available addresses: 15

Available Addresses:
2001:db8::db8:800:200c:417a
2001:db8::db8:800:200c:417b
2001:db8::db8:800:200c:417c
2001:db8::db8:800:200c:417d
2001:db8::db8:800:200c:417e
2001:db8::db8:800:200c:417f
2001:db8::db8:800:200c:4180
2001:db8::db8:800:200c:4181
2001:db8::db8:800:200c:4182
```

```
2001:db8::db8:800:200c:4183
2001:db8::db8:800:200c:4184
2001:db8::db8:800:200c:4185
2001:db8::db8:800:200c:4186
2001:db8::db8:800:200c:4187
2001:db8::db8:800:200c:4188
```

関連コマンド

コマンド	説明
ipv6 local pool	IPv6 アドレス プールを設定します。

show ipv6 mld traffic

Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）トラフィック カウンタ情報を表示するには、特権 EXEC モードで **show ipv6 mld traffic** コマンドを使用します。

show ipv6 mld traffic

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが追加されました。

使用上のガイドライン

show ipv6 mld traffic コマンドを使用すると、予期される数の MLD メッセージが受信および送信されたかどうかをチェックできます。

show ipv6 mld traffic コマンドで提供される情報は次のとおりです。

- Elapsed time since counters cleared：カウンタがクリアされてからの経過時間。
- Valid MLD Packets：送受信された有効な MLD パケットの数。
- Queries：送受信された有効なクエリーの数。
- Reports：送受信された有効なレポートの数。
- Leaves：送受信された有効な脱退の数。
- Mtraee packets：送受信されたマルチキャスト トレース パケットの数。
- Errors：発生したエラーのタイプと数。

例

次に、**show ipv6 mld traffic** コマンドの出力例を示します。

```
ciscoasa# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
```

```
                    Received            Sent
Valid MLD Packets   1                   3
Queries             1                   0
Reports             0                   3
Leaves              0                   0
Mtrace packets      0               0
Errors:
Malformed Packets   0
Martian source      0
Non link-local source 0
Hop limit is not equal to 1 0
```

関連コマンド

コマンド	説明
clear ipv6 mld traffic	すべての MLD トラフィック カウンタをリセットします。

show ipv6 neighbor

IPv6 ネイバー探索キャッシュ情報を表示するには、特権 EXEC モードで **show ipv6 neighbor** コマンドを使用します。

show ipv6 neighbor [*if_name* | *address*]

構文の説明

address	(任意)指定された IPv6 アドレスについてのみネイバー探索キャッシュ情報を表示します。
if_name	(オプション)**nameif** コマンドで設定された指定のインターフェイス名についてのみキャッシュ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show ipv6 neighbor コマンドで提供される情報は次のとおりです。

- IPv6 Address:ネイバーまたはインターフェイスの IPv6 アドレス。
- Age:アドレスが到達可能と確認されてからの経過時間(分単位)。ハイフン(-)はスタティック エントリを示します。
- Link-layer Addr:MAC アドレス。アドレスが不明の場合、ハイフン(-)が表示されます。
- State:ネイバー キャッシュ エントリの状態。

(注) 到達可能性検出は IPv6 ネイバー探索キャッシュのスタティック エントリに適用されないため、INCMP(不完全)状態と REACH(到達可能)状態の記述は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。

次に、IPv6 ネイバー探索キャッシュのダイナミック エントリについて表示される可能性のある状態を示します。

- INCMP:（不完全）エントリに対してアドレス解決を実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージが受信されていません。
- REACH:（到達可能）ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以内に受信されました。REACH 状態になっている間は、パケットが送信されるときにデバイスは特別なアクションを実行しません。
- STALE:転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が、ReachableTime ミリ秒を超えています。STALE 状態になっている間は、パケットが送信されるまでデバイスはアクションを実行しません。
- DELAY:転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が、ReachableTime ミリ秒を超えています。パケットは直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。DELAY 状態に入ってから、DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が PROBE に変更されます。
- PROBE:到達可能性確認が受信されるまで、RetransTimer ミリ秒ごとに、ネイバー要請メッセージを再送信することで、到達可能性確認が積極的に求められます。
- ????:不明な状態。

次に、IPv6 ネイバー探索キャッシュのスタティック エントリについて表示される可能性のある状態を示します。

- INCMP:（不完全）このエントリのインターフェイスはダウンしています。
- REACH:（到達可能）このエントリのインターフェイスは動作しています。

- インターフェイス
  アドレスに到達可能であったインターフェイス。

例

次に、インターフェイスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
ciscoasa# show ipv6 neighbor inside
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                  0 0003.a0d6.141e  REACH inside
3001:1::45a                               - 0002.7d1a.9472  REACH inside
```

次に、IPv6 アドレスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
ciscoasa# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH inside
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。
ipv6 neighbor	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。

show ipv6 ospf

OSPFv3 ルーティング プロセスに関する一般情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf** コマンドを使用します。

show ipv6 ospf [*process_id*] [*area_id*]

構文の説明

area_id	（オプション）指定したエリアに関する情報だけを表示します。
process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPFv3 ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show ipv6 ospf コマンドは次の設定を表示します。

- イベント ログ機能
- ルータ タイプ
- 再配布ルート タイプ
- SPF schedule delay
- 連続する 2 つの SPF 間のホールド時間
- 連続する 2 つの SPF 間の待機時間
- Minimum LSA interval
- Minimum LSA arrival

例

次に、**show ipv6 ospf** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

関連コマンド

コマンド	説明
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。
show ipv6 ospf database	特定のルータの OSPFv3 データベースに関係する情報の一覧を表示します。

show ipv6 ospf border-routers

エリア境界ルータ（ABR）および自律システム境界ルータ（ASBR）に対して、OSPFv3 ルーティング テーブル エントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf border-routers** コマンドを使用します。

show ipv6 ospf [*process_id*] **border-routers**

構文の説明

process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPFv3 ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show ipv6 ospf border-routers コマンドは次の設定を表示します。

- エリア内ルート
- エリア間ルート
- IPv6 アドレス
- インターフェイス タイプ
- Area ID
- SPF 番号

例

次に、**show ipv6 ospf border-routers** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf database	特定のルータの OSPFv3 データベースに関係する情報の一覧を表示します。

show ipv6 ospf database

特定のルータの OSPFv3 データベースに関連する情報のリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf database** コマンドを使用します。

show ipv6 ospf [*process_id*] [*area_id*] **database** [**external | inter-area prefix | inter-area-router | network | nssa-external | router | area | as | ref-lsa |** [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] **| self-originate**] [**internal**] [**database-summary**]

構文の説明

adv-router *router-id*	(オプション)アドバタイズするルータのすべての LSA を表示します。ルータ ID は、RFC 2740 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
area	(オプション)エリア LSA に関する情報だけを表示します。
area_id	(オプション)指定したエリアに関する情報だけを表示します。
as	(オプション)不明な自律システム(AS)LSA をフィルタリングします。
database-summary	(オプション)データベースと全体にある各エリアの各 LSA タイプの数を表示します。
destination-router-id	(オプション)指定した宛先ルータに関する情報だけを表示します。
external	(任意)外部 LSA の情報だけを表示します。
interface	(オプション)インターフェイス コンテキストでフィルタリングされた LSA に関する情報を表示します。
interface-name	(オプション)LSA のインターフェイス名を指定します。
internal	(オプション)内部 LSA の情報だけを表示します。
inter-area prefix	(オプション)エリア間プレフィックスに基づいた LSA の情報だけを表示します。
inter-area router	(オプション)エリア間ルータ LSA 基づいた LSA の情報だけを表示します。
link	(オプション)リンク LSA に関する情報を表示します。これが **unknown** キーワードに従う場合、**link** キーワードでリンクスコープ LSA がフィルタリングされます。
link-state-id	(オプション)LSA を区別するために使用する整数を指定します。ネットワーク LSA およびリンク LSA では、リンクステート ID はインターフェイス インデックスに一致します。
network	(オプション)ネットワーク LSA に関する情報を表示します。
nssa-external	(オプション)Not-So-Stubby-Area(NSSA)の外部 LSA に関する情報だけを表示します。
prefix *ipv6-prefix*	(オプション)ネイバーのリンクローカル IPv6 アドレスを表示します。IPv6 プレフィックスは、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
process_id	(オプション)ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
ref-lsa	(オプション)プレフィックス LSA タイプをさらにフィルタリングします。

ルータ	（オプション）ルータ LSA に関する情報を表示します。
self-originate	（オプション）ローカル ルータから自己生成 LSA だけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、さまざまな形式で、異なる OSPFv3 LSA に関する情報を提供します。

例

次に、**show ipv6 ospf database** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3
```

```
            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf events

OSPFv3 内部イベント情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf events** コマンドを使用します。

show ipv6 ospf [*process_id*] **events** [*type*]

構文の説明

process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
type	（オプション）表示するイベント タイプのリスト。タイプを 1 つ以上指定しないと、すべてのイベントが表示されます。次のタイプでフィルタリングできます。 • **generic**：一般的なイベント。 • **interface**：インターフェイス状態変化イベント。 • **lsa**：LSA 到着イベントおよび LSA 生成イベント。 • **neighbor**：ネイバー状態変化イベント。 • **reverse**：逆の順序でイベントを表示。 • **rib**：ルータ情報ベースの更新イベント、削除イベント、および再配布イベント。 • **spf**：SPF のスケジューリング イベントおよび SPF 実行イベント。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、**show ipv6 ospf events** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf events

OSPFv3 Router with ID (10.1.3.2) (Process ID 10)

   1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
   2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,
   Seq# 80000008, Age 1, Area 10
   3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004, Age
   0, Area 10
   4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,
   Age 0, Area 10
   5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
   6 Jul 9  18:41:18.902: Starting External processing in area 10
   7 Jul 9  18:41:18.902: Starting External processing
   8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
   9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
  10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
  11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
  12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
  13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
  14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
  15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0, Adv-Rtr
  50.100.168.192
  16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
  Seq# 80000003, Age 1, Area 10
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf flood-list

インターフェイスを介してフラッディングされるのを待機している OSPFv3 LSA のリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf flood-list** コマンドを使用します。

show ipv6 ospf [*process_id*] [*area_id*] **flood-list** *interface-type interface-number*

構文の説明

area_id	(オプション)指定したエリアに関する情報だけを表示します。
interface-number	(オプション)LSA がフラッディングされるインターフェイス番号を指定します。
interface-type	(オプション)LSA がフラッディングされるインターフェイス タイプを指定します。
process_id	(オプション)ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPFv3 ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 パケット ペーシング情報を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf flood-list** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
```

```
Link state retransmission due in 14 msec

Type    LS ID           ADV RTR         Seq NO      Age    Checksum
0x2001  0               172.16.6.6      0x80000031  0      0x1971

Interface FastEthernet0/0, Queue length 0

Interface ATM3/0, Queue length 0
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf graceful-restart

OSPFv3 グレースフル リスタートに関する情報を表示するには、特権 EXEC モードで **show ipv6 ospf graceful-restart** コマンドを使用します。

show ipv6 ospf graceful-restart

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

例

次に、**show ipv6 ospf graceful-restart** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。

show ipv6 ospf interface

OSPFv3 関連のインターフェイス情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf interface** コマンドを使用します。

show ipv6 ospf [*process_id*] [*area_id*] **interface** [*type-number*] [**brief**]

構文の説明

area_id	（オプション）指定したエリアに関する情報だけを表示します。
brief	（オプション）OSPFv3 インターフェイス、状態、アドレスとマスク、およびルータのエリアに関する簡単な概要情報を表示します。
process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
type-number	（オプション）インターフェイスのタイプおよび番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 インターフェイス、状態、アドレスとマスク、およびルータのエリアに関する概要情報を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf interface** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf interface

ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
```

```
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf neighbor

インターフェイスごとの OSPFv3 ネイバー情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf neighbor** コマンドを使用します。

show ipv6 ospf [*process_id*] [*area_id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

構文の説明

area_id	（オプション）指定したエリアに関する情報だけを表示します。
detail	（オプション）すべてのネイバーの詳細情報を表示します。
interface-type interface-number	（オプション）インターフェイスのタイプおよび番号を指定します。
neighbor-id	（オプション）ネイバー ID を指定します。
process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスごとの OSPFv3 ネイバー情報を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf neighbor** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
172.16.4.4       1    FULL/  -        00:00:31    14              POS4/0
172.16.3.3       1    FULL/BDR        00:00:30    3               FastEthernet00
172.16.5.5       1    FULL/  -        00:00:33    13              ATM3/0
```

次に、**show ipv6 ospf neighbor detail** コマンドの出力例を示します。

```
Neighbor 172.16.4.4
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63AD1B0D
    Dead timer due in 00:00:33
    Neighbor is up for 00:48:56
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.3.3
    In the area 1 via interface FastEthernet0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 00:00:33
    Neighbor is up for 00:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.5.5
    In the area 2 via interface ATM3/0
    Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63F7D249
    Dead timer due in 00:00:38
    Neighbor is up for 00:10:01
    Index 1/1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf request-list

ルータによって要求されたすべての LSA のリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf request-list** コマンドを使用します。

show ipv6 ospf [*process_id*] [*area_id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

構文の説明

area_id	(オプション)指定したエリアに関する情報だけを表示します。
interface	(オプション)このインターフェイスからルータにより要求されるすべての LSA のリストを指定します。
interface-neighbor	(オプション)このネイバーのインターフェイスのルータにより要求されるすべての LSA のリストを指定します。
neighbor	(オプション)このネイバーからルータにより要求されるすべての LSA のリストを指定します。
process_id	(オプション)ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ルータが要求するすべての LSA を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf request-list** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf request-list


           OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
  2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
  2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf retransmission-list

再送信を待機しているすべての LSA のリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf retransmission-list** コマンドを使用します。

show ipv6 ospf [*process_id*] [*area_id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

構文の説明

area_id	(オプション)指定したエリアに関する情報だけを表示します。
interface	(オプション)このインターフェイスで再送信を待機しているすべての LSA のリストを指定します。
interface-neighbor	(オプション)このネイバーからこのインターフェイスの再送信を待機しているすべての LSA のリストを表示します。
neighbor	(オプション)このネイバーの再送信を待機しているすべての LSA のリストを指定します。
process_id	(オプション)ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

再送信を待機しているすべての LSA を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf retransmission-list** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf retransmission-list


        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf statistic

さまざまな OSPFv3 統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf statistic** コマンドを使用します。

show ipv6 ospf [*process_id*] **statistic** [**detail**]

構文の説明

detail	（オプション）トリガー ポイントを含む詳細な SPF 情報を指定します。
process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

SPF が実行された回数、原因、および期間を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf statistic** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf 10 statistic detail


Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
```

```
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf summary-prefix

OSPFv3 プロセスに設定されたすべてのサマリー アドレス再配布情報のリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf summary-prefix** コマンドを使用します。

show ipv6 ospf [*process_id*] **summary-prefix**

構文の説明

process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 プロセスに設定されたすべてのサマリー アドレス再配布情報のリストを表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf summary-prefix** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf timers

OSPFv3 タイマー情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf timers** コマンドを使用します。

show ipv6 ospf [*process_id*] **timers** [**lsa-group | rate-limit**]

構文の説明

lsa-group	（オプション）OSPFv3 LSA グループ情報を指定します。
process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
rate-limit	（オプション）OSPFv3 LSA のレート制限情報を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 プロセスで設定されている LSA 情報を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf timers lsa-group** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf timers lsa-group

OSPFv3 Router with ID (10.10.13.101) (Process ID 1)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
```

```
Index 3 Timestamp 97293
Index 4 Timestamp 97548

Failure Head 0, Last 0 LSA group failure logged

            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546

Failure Head 0, Last 0 LSA group failure logged
```

次に、**show ipv6 ospf timers rate-limit** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf timers rate-limit

List of LSAs that are in rate limit Queue
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf traffic

現在使用可能なインターフェイスの OSPFv3 トラフィック関連の統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf traffic** コマンドを使用します。

show ipv6 ospf [*process_id*] **traffic** [*interface_name*]

構文の説明

interface_name	（オプション）インターフェイスの名前（インターフェイス GigabitEthernet0/0 など）を指定します。特定のインターフェイスにトラフィックを分離するには、このオプションを使用します。
process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

使用可能なインターフェイスの OSPFv3 トラフィック関連情報を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf traffic** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf 10 traffic inside

Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid                       0 0
```

```
RX Hello                       1232 53132
RX DB des                        27 896
RX LS req                         3 216
RX LS upd                        28 2436
RX LS ack                        14 1064
RX Total                       1304 57744

TX Failed                         0 0
TX Hello                        753 32072
TX DB des                        27 1056
TX LS req                         2 92
TX LS upd                         9 1128
TX LS ack                        15 900
TX Total                        806 35248
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf virtual-links

OSPFv3 仮想リンクのパラメータと現在の状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf virtual-links** コマンドを使用します。

show ipv6 ospf virtual-links

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 仮想リンクのパラメータと現在の状態を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf virtual-links** コマンドの出力例を示します。

```
ciscoasa# show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 prefix-list

設定された IPv6 プレフィックス リストに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 prefix-list** コマンドを使用します。

show ipv6 prefix-list [**summary** | **detail**] [*policy_list_name* [**seq** *sequence_number* | *network/length* [**longer** | **first-match**]]]

構文の説明

policy_list_name	(オプション)指定されたポリシー リストに関する情報を表示します。
summary	(オプション)要約された追加統計情報を表示します。
detail	(オプション)要約された追加統計情報とプレフィックス リストのエントリを表示します。
seq *sequence_number*	(オプション)指定されたプレフィックス リストに指定されたシーケンス番号を持つプレフィックス リストのエントリだけを表示します。
network/length [**longer** | **first-match**]	(オプション)このネットワーク アドレスおよびプレフィックス長(ビット単位)を使用する、指定されたプレフィックス リストのすべてのエントリを表示します。 次のキーワードを追加することで、一致条件を変更できます。 • **longer**:指定された network/length と一致するか、または(より限定的な)指定されたプレフィックス リストのエントリすべてを表示します。 • **first-match**:指定された network/length と一致する、指定されたプレフィックス リストの最初のエントリを表示します。

デフォルト

プレフィックス リストの名前を指定しない場合、このコマンドはすべてのプレフィックス リストを表示します。他のキーワードを含めない場合、出力にはプレフィックス リストのエントリだけが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

ルート マップとポリシー リストの一致基準としてルーティングでプレフィックス リストを使用します。

例

次に、**show ipv6 prefix-list** コマンドの出力例を示します。

```
ciscoasa(config)# show ipv6 prefix-list
ipv6 prefix-list test-ipv6-prefix: 1 entries
   seq 5 permit 2001:db8:0:cd30::/64
```

次に、要約された出力の例を示します。

```
ciscoasa(config)# show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

次に、詳細な出力の例を示します。

```
ciscoasa(config)# show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2

   seq 5 permit 2001:db8:0:cd30::/64 (hit count: 0, refcount: 1)
```

関連コマンド

コマンド	説明
ipv6 prefix-list	IPv6 プレフィックス リストを設定します。

show ipv6 route management-only

IPv6 ルーティング テーブルの内容を表示するには、特権 EXEC モードで **show ipv6 route** コマンドを使用します。management-only キーワードは、IPv6 管理ルーティング テーブル内のルートを表示します。

show ipv6 route management-only [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]

構文の説明

managment-only	IPv6 管理ルーティング テーブル内のルートを表示します。
クラスタ	（オプション）クラスタ内の IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。
フェールオーバー	（オプション）IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。
interface	（オプション）IPv6 インターフェイス固有のルートを表示します。
ospf	（オプション）OSPFv3 ルートを表示します。
summary	（オプション）IPv6 ルート集約を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	**failover**、**cluster**、**ospf**、**interface** および **summary** キーワードのサポートが追加されました。
9.5(1)	管理ルーティング テーブル機能のサポートが追加されました。

使用上のガイドライン

IPv6 専用の情報である点を除いて、**show ipv6 route** コマンドの出力は、**show route** コマンドと類似しています。

次に、IPv6 ルーティング テーブルに表示される情報を示します。

- Codes:ルートを生成したプロトコルを示します。表示される値は次のとおりです。
  - C:接続済み
  - L:ローカル
  - S:スタティック
  - R:RIP 生成
  - B:BGP 生成
  - I1:ISIS L1:統合 IS-IS Level 1 生成
  - I2:ISIS L2:統合 IS-IS Level 2 生成
  - IA:ISIS エリア間:統合 IS-IS エリア間生成
- fe80::/10:リモート ネットワークの IPv6 プレフィックスを示します。
- [0/0]:カッコ内の最初の数値は情報ソースのアドミニストレーティブ ディスタンスです。2 番目の数値はルートのメトリックです。
- via ::::リモート ネットワークへの次のルータのアドレスを指定します。
- inside:指定されたネットワークへの次のルータに到達できるインターフェイスを指定します。

(注) ASA で対応する機能が設定されていない場合、**clustering** および **failover** キーワードは表示されません。

例

次に、**show ipv6 route** コマンドの出力例を示します。

```
ciscoasa# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

次に、**show ipv6 route failover** コマンドの出力例を示します。

```
ciscoasa# show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired

O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

次に、マスター ユニットでの **show ipv6 route cluster** コマンドの出力例を示します。

```
ciscoasa/LB1/master(config)# show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

次に、ロール変更時のスレーブ ユニットでの **show ipv6 route cluster** コマンドの出力例を示します。

```
ciscoasa/LB2/slave(config)# cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
ciscoasa/LB2/slave(config)#
ciscoasa/LB2/master(config)#
ciscoasa/LB2/master(config)# show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 ルーティング テーブルの更新およびルート キャッシュの更新に関するデバッグ メッセージを表示します。
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 routers

オンリンク ルータから受信した IPv6 ルータ アドバタイズメント情報を表示するには、特権 EXEC モードで **show ipv6 routers** コマンドを使用します。

show ipv6 routers [*if_name*]

構文の説明

if_name	(任意)情報を表示する対象となる、**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

例

次に、インターフェイス名を指定せずに入力した **show ipv6 routers** コマンドの出力例を示します。

```
ciscoasa# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

関連コマンド

コマンド	説明
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 traffic

IPv6 トラフィックの統計情報を表示するには、特権 EXEC モードで **show ipv6 traffic** コマンドを使用します。

show ipv6 traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

トラフィック カウンタをクリアするには、**clear ipv6 traffic** コマンドを使用します。

例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
```

```
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

関連コマンド

コマンド	説明
clear ipv6 traffic	IPv6 トラフィック カウンタをクリアします。

show isakmp ipsec-over-tcp stats コマンド～ show mroute コマンド

show isakmp ipsec-over-tcp stats

IPsec over TCP の実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp ipsec-over tcp stats** コマンドを使用します。

show isakmp ipsec-over-tcp stats

構文の説明　このコマンドには引数またはキーワードはありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
ASAv(1)	**show isakmp ipsec-over-tcp stats** コマンドが追加されました。
7.2(1)	**show isakmp ipsec-over-tcp stats** コマンドは廃止されました。**show crypto isakmp ipsec-over-tcp stats** コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets
- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures
- Checksum errors
- Internal errors

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
ciscoasa(config)# show isakmp ipsec-over-tcp stats
Global IPsec over TCP Statistics
--------------------------------
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
crypto isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp sa** コマンドを使用します。

show isakmp sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp sa** コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE Peer	タイプ	Dir	Rky	状態
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE Peer	タイプ	Dir	Rky	状態	Encrypt	Hash	認証	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
ciscoasa(config)# show isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp stats

実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp stats** コマンドを使用します。

show isakmp stats

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
ASAv(1)	**show isakmp stats** コマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp stats** コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

各カウンタは、関連する cikePhase1GW カウンタにマッピングします。これらのカウンタの詳細については、「CISCO-IPSEC-FLOW-MONITOR-MIB.my」を参照してください。

- Active/Standby Tunnels：cikePhase1GWActiveTunnels
- Previous Tunnels：cikePhase1GWPreviousTunnels
- In Octets：cikePhase1GWInOctets
- In Packets：cikePhase1GWInPkts
- In Drop Packets：cikePhase1GWInDropPkts
- In Notifys：cikePhase1GWInNotifys
- In P2 Exchanges：cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids：cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects：cikePhase1GWInP2ExchgRejects

- In P2 Sa Delete Requests : cikePhase1GWInP2SaDelRequests
- Out Octets : cikePhase1GWOutOctets
- Out Packets : cikePhase1GWOutPkts
- Out Drop Packets : cikePhase1GWOutDropPkts
- Out Notifys : cikePhase1GWOutNotifys
- Out P2 Exchanges : cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids : cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects : cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests : cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels : cikePhase1GWInitTunnels
- Initiator Fails : cikePhase1GWInitTunnelFails
- Responder Fails : cikePhase1GWRespTunnelFails
- System Capacity Fails : cikePhase1GWSysCapFails
- Auth Fails : cikePhase1GWAuthFails
- Decrypt Fails : cikePhase1GWDecryptFails
- Hash Valid Fails : cikePhase1GWHashValidFails
- No Sa Fails : cikePhase1GWNoSaFails

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails

- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
ciscoasa(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isis database

IS-IS リンクステート データベースを表示するには、特権 EXEC モードで **show isis database** コマンドを使用します。

show isis database [{**detail** | **verbose**} [**ip** [**unicast**] | **ipv6** [**unicast**]] [**topology base**]] [**level-1** | **level-2**]

構文の説明

level-1	(任意) レベル 1 の IS-IS リンクステート データベースを示します。
level-2	(任意) レベル 2 の IS-IS リンクステート データベースを示します。
ip	(オプション) IPv4 アドレスファミリの IS-IS リンクステート データベースを表示します。
ipv6	(オプション) IPv6 アドレスファミリの IS-IS リンクステート データベースを表示します。
detail	(任意) 各リンクステート パケット (LSP) のコンテンツを表示します。
verbose	(オプション) IS-IS データベースに関する追加情報を表示します。
topology base	(オプション) MTR トポロジを表示します。
unicast	(オプション) ユニキャスト アドレス ファミリを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IS-IS リンクステート データベースを表示します。

例

次に、**show isis database** コマンドの出力例を示します。

```
ciscoasa# show isis database

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d300     0x3d0d              674                0/0/0
routerA.00-00     0x1b541556     0xa349              928                0/0/0
c3.00-00              0x9257c979     0x9952              759                0/0/0
c2.00-00             *0xef11e977     0x3188              489                0/0/0
c2.01-00             *0xa8333f03     0xd6ea              829                0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f24      0xaba2              526                0/0/0
routerA.00-00     0x0d540b55      0x81d7              472                0/0/0
routerA.00-01     0xffffff01          0xe20b              677                0/0/0
c3.00-00              0x002e5434      0xb20a              487                0/0/0
c2.00-00             *0x74fd1227      0xbb0f              742                0/0/0
c2.01-00             *0x7ee72c1a      0xb506              968                0/0/0
```

表 9-1　show isis database のフィールド

フィールド	説明
LSPID	LSP の ID。最初の 6 オクテットは、LSP を生成したルータのシステム ID を形成します。 次のオクテットは疑似ノード ID です。このバイトが非ゼロの場合、LSP はシステムからのリンクを記述します。ゼロの場合は、LSP は、いわゆる非疑似ノード LSP です。このメカニズムは、Open Shortest Path First（OSPF）プロトコルのルータ リンクステート アドバタイズメント（LSA）に類似しています。LSP は、送信元ルータの状態を記述します。 各 LAN に対して、その LAN の指定ルータは疑似ノード LSP の作成およびフラッドを行い、その LAN に接続されたすべてのシステムを記述します。 最後のオクテットは LSP 番号です。単一の LSP に収容可能な量を超えるデータがある場合は、LSP は複数の LSP フラグメントに分割されます。各フラグメントには、異なる LSP 番号が割り当てられます。アスタリスク（*）は、その LSP が、このコマンドの送信元のシステムによって生成されたことを示します。
LSP Seq Num	他のシステムが発信元から最新情報を受信しているか判断できる、LSP のシーケンス番号。
LSP Checksum	LSP パケットのチェックサム。
LSP Holdtime	LSP が有効である時間（秒単位）。LSP Holdtime がゼロである場合は、LSP がパージされて、すべてのルータのリンクステート データベース（LSDB）から削除されていることを示します。この値は、パージされた LSP が、完全に削除されるまでに LSDB 内に存在する時間を示します。
ATT	Attach ビット。このビットは、そのルータがレベル 2 ルータでもあるため、他のエリアに到達できることを示します。レベル 1 だけのルータ、および他のレベル 2 ルータとの接続を失ったレベル 1-2 ルータは、Attach ビットを使用して最も近いレベル 2 ルータを検出します。ルータは、最も近いレベル 2 ルータへのデフォルト ルートを示します。

表 9-1　show isis database のフィールド（続き）

フィールド	説明
P	P ビット。中継システムが修復可能なエリア パーティションであるかどうかを検出します。シスコおよび他のベンダーは、エリア パーティション修復をサポートしません。
OL	過負荷ビット。IS が混雑しているかどうかを判断します。過負荷ビットがセットされると、他のルータは、ルータを計算しているときに中継ルータとしてこのシステムを使用しません。過負荷になっているルータに直接接続された宛先のパケットだけが、このルータに送信されます。

次に、**show isis database detail** コマンドの出力例を示します。出力に示されるように、**show isis database** コマンドで表示される情報に加えて、**show isis database detail** コマンドにより各 LSP のコンテンツが表示されます。

```
ciscoasa# show isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d301      0x3b0e               1189                     0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00      0x1b541556     0xa349                642                      0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

表 9-2　show isis database detail のフィールド

フィールド	説明
Area Address	ルータから到達可能なエリア アドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリア アドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリア アドレスになります。
メトリック	送信側ルータとアドバタイズされたネイバー間の隣接関係のコスト用の IS-IS メトリック、またはアドバタイズ元のルータからアドバタイズ対象の宛先（IP アドレス、エンド システム [ES]、または CLNS プレフィックス）に到達するコスト用のメトリック。

次に、**show isis database detail** コマンドの、別の出力例を示します。この LSP は、レベル 2 LSP です。エリア アドレス 39.0001 は、ルータが存在するエリアのアドレスです。

```
ciscoasa# show isis database 12 detail

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f25      0xa9a3               1076                     0/0/0
  Area Address: 49.0001
```

```
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IS c2.01
routerA.00-00     0x0d540b56     0x7fd8                 941                       0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IS c2.01
  Metric:          0 IP-External 1.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.2.2.0 255.255.255.0
  Metric:          0 IP-External 3.1.1.0 255.255.255.0
```

次に、**show isis database verbose** コマンドの出力例を示します。

```
ciscoasa# show isis database verbose

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00            *0xea19d301   0x3b0e        644               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   22.22.22.1
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00         0x1b541557   0xa14a        783               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   22.22.22.5
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

表 9-3　show isis database verbose のフィールド

フィールド	説明
LSPID	リンクステート パケット（LSP）ID。最初の 6 オクテットは、LSP を生成したルータのシステム ID を形成します。 次のオクテットは疑似ノード ID です。このバイトがゼロの場合は、LSP はシステムからのリンクを記述します。ゼロでない場合は、LSP は非疑似ノード LSP です。これは、Open Shortest Path First（OSPF）のルータ LSA と類似しており、LSP は送信元ルータの状態を記述します。各 LAN に対して、その LAN の指定ルータは疑似ノード LSP の作成およびフラッドを行い、その LAN に接続されたすべてのシステムを記述します。 最後のオクテットは LSP 番号です。すべてのデータが単一の LSP に収容できない場合は、その LSP は複数の LSP フラグメントに分割されます。各フラグメントには、異なる LSP 番号が割り当てられます。アスタリスク（*）は、このコマンドを送信したシステムが LSP を生成したことを示します。
LSP Seq Num	他のシステムが発信元から最新情報を受信しているか判断できる、LSP のシーケンス番号。
LSP Checksum	LSP パケットのチェックサム。

表 9-3　show isis database verbose のフィールド(続き)

フィールド	説明
LSP Holdtime	LSP が有効である時間(秒単位)。LSP Holdtime がゼロである場合は、LSP がパージされて、すべてのルータのリンクステート データベース(LSDB)から削除されていることを示します。この値は、パージされた LSP が、完全に削除されるまでに LSDB 内に存在する時間を示します。
ATT	Attach ビット。このビットは、そのルータがレベル 2 ルータでもあるため、他のエリアに到達できることを示します。レベル 1 ルータは、Attach ビットを使用して、最も近いレベル 2 ルータを検出します。ルータは、最も近いレベル 2 ルータへのデフォルト ルートを設定します。
P	P ビット。このビットは、IS がエリア パーティションを修復できるかどうかを検出します。シスコおよび他のベンダーは、エリア パーティション修復をサポートしません。
OL	過負荷ビット。このビットは、IS が混雑しているかどうかを判断します。過負荷ビットがセットされると、他のルータは、ルータを計算しているときに、中継ルータとしてこのシステムを使用しません。過負荷になっているルータに直接接続された宛先のパケットだけが、このルータに送信されます。
Area Address	ルータから到達可能なエリア アドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリア アドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリア アドレスになります。
NLPID	ネットワーク層プロトコル ID。
Hostname	ノードのホスト名。
ルータ ID	ノードのトラフィック エンジニアリング ルータ ID。
IP Address	インターフェイスの IPv4 アドレス。
メトリック	発信元ルータとアドバタイズされるネイバー間の隣接のコストの IS-IS メトリック、またはアドバタイズするルータからアドバタイズされる宛先までにかかるコストのメトリック(IP アドレス、エンド システム(ES)、またはコネクションレス型ネットワーク サービス(CLNS)のプレフィックスを指定できます)。
アフィニティ	フラッドされているリンク属性フラグ。
Physical BW	リンクの帯域幅容量(ビット/秒)。
Reservable BW	このリンクの予約可能帯域幅。
BW Unreserved	予約可能帯域幅。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。

コマンド	説明
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis hostname

IS-IS ルータのルータ名とシステム ID のマッピング テーブル エントリを表示するには、特権 EXEC モードで **show isis hostname** コマンドを使用します。

show isis hostname

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

IS-IS ルーティング ドメインでは、各ルータはシステム ID により表されます。システム ID は、IS-IS ルータごと構成されている Network Entity Title（NET）の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されているルータのシステム ID が 0023.0003.000a であるとします。ネットワーク管理者にとって、ルータでのメンテナンスやトラブルシューティングの間、ルータ名とシステム ID の対応を覚えているのは難しいことです。**show isis hostname** コマンドを入力すると、ルータ名とシステム ID のマッピング テーブルに含まれるエントリが表示されます。

no hostname dynamic コマンドを入力してダイナミック ホスト名機能が無効にされていない場合は、マッピングはダイナミック ホスト マッピング テーブルで構成されます。

例

次に、ciscoASA のホスト名を変更し、NET 49.0001.0050.0500.5005.00 を ciscoASA に割り当てる例を示します。

```
ciscoasa(config)# hostname ciscoASA
ciscoASA(config)# router isis
ciscoASA(config-router)# net 49.0001.0050.0500.5005.00
ciscoASA(config-router)# hostname dynamic
ciscoASA(config-router)#
```

show isis hostname コマンドを入力すると、ダイナミック ホスト マッピング テーブルが表示されます。ダイナミック ホスト マッピング テーブルは、ciscoASA、c2、c3 および routerA という名前のローカル ルータの、ルータ名とシステム ID のマッピング テーブル エントリを表示します。このテーブルは、c3 がレベル-1 ルータであり、そのホスト名がレベル-1(L1)リンクステート プロトコル(LSP)によりアドバタイズされることも示します。c2 はレベル-2 ルータであり、そのホスト名は L2 LSP によりアドバタイズされます。ASA ciscoASA のレベルの下に表示される * 記号は、これが、ASA のルータ名とシステム ID のマッピング情報であることを示します。

```
ciscoASA# show isis hostname

Level  System ID       Dynamic Hostname  (c1)
     * 0050.0500.5005   ciscoASA
    1  0050.0500.5007   c3
    2  0050.0500.5006   routerA
    2  0050.0500.5008   c2
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される(受信ではなく)IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。

コマンド	説明
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis lsp-log

新しい LSP をトリガーしたインターフェイスの、レベル 1 およびレベル 2 の IS-IS リンクステート パケット（LSP）ログを表示するには、特権 EXEC モードで **show isis lsp-log** コマンドを使用します。

show isis lsp-log

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

新しい LSP をトリガーしたインターフェイスのレベル 1 およびレベル 2 の IS-IS リンクステート パケット（LSP）のログを表示します。

例

次に、**show isis lsp-log** コマンドの出力例を示します。

```
ciscoasa# show isis lsp-log

   Level 1 LSP log
 When       Count       Interface         Triggers
 04:16:47     1         subint             CONFIG NEWADJ DIS
 03:52:42     2         subint             NEWADJ DIS
 03:52:12     1         subint             ATTACHFLAG
 03:31:41     1         subint             IPUP
 03:30:08     2         subint             CONFIG
 03:29:38     1         subint             DELADJ
 03:09:07     1         subint             DIS ES
 02:34:37     2         subint             NEWADJ
 02:34:07     1         subint             NEWADJ DIS
```

```
  Level 2 LSP log
When       Count       Interface         Triggers
03:09:27     1         subint             CONFIG NEWADJ
03:09:22     1         subint             NEWADJ
02:34:57     2         subint             DIS
02:34:50     1                                IPUP
02:34:27     1         subint             CONFIG DELADJ
02:13:57     1         subint             DELADJ
02:13:52     1         subint             NEWADJ
01:35:58     2         subint             IPIA
01:35:51     1                               AREASET IPIA
```

表 9-4　show isis lsp-log のフィールド

フィールド	説明
When	LSP が生成されてからの経過時間。
Count	このときに発生したイベントの数。
インターフェイス	LSP を再び生成したインターフェイス。
Triggers	LSP のフラッドをトリガーしたイベント。次のような、LSP に可能なトリガー。 • AREASET：アクティブ エリア セットが変更されました。 • ATTACHFLAG：Attach ビットの状態が変更されました。 • CLEAR：ある形式の手動の clear コマンドが送信されました。 • CONFIG：任意のコンフィギュレーションが変更されました。 • DELADJ：隣接関係がダウンしました。 • DIS：DIS が変更されたか、または疑似ノードが変更されました。 • ES：エンド システムの隣接関係が変更されました。 • HIPPITY：LSPDB 過負荷ビットの状態が変更されました。 • IF_DOWN：新しい LSP が必要です。 • IP_DEF_ORIG：元のデフォルト情報が変更されました。 • IPDOWN：直接接続されている IP プレフィックスがダウンしました。 • IP_EXTERNAL：再配布された IP ルートが現れたか、または失われました。 • IPIA：エリア間 IP ルートが現れたか、または失われました。 • IPUP：直接接続されている IP プレフィックスが起動しました。 • NEWADJ：新しい隣接関係が現れました。 • REDIST：再配信されたレベル-2 CLNS ルートが変更されました。 • RRR_INFO：RRR 帯域幅リソース情報。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。

コマンド	説明
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。

コマンド	説明
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis neighbors

IS-IS ネイバーに関する情報を表示するには、特権 EXEC モードで **show isis neighbors** コマンドを使用します。

show isis neighbors [**detail**]

構文の説明

detail	（任意）IS-IS ネイバーの詳細情報を表示します。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォールモード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

show isis neighbors コマンドは、接続されている IS-IS ルータに関する簡潔な情報を表示するために使用されます。**detail** キーワードを入力すると、さらに詳細な情報が表示されます。

例

show isis neighbors command を入力して、IS-IS ネイバーの routerA に関する情報を表示します。

```
ciscoasa# show isis neighbors

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint        22.22.22.5        UP    21             c2.01
routerA          L2    subint        22.22.22.5        UP    22             c2.01
c2                   L1    subint        22.22.22.3        UP     9              c2.01
c2                 L2    subint       22.22.22.3       UP     9            c2.01
```

show isis neighbors detail コマンドを入力して、IS-IS ネイバーの routerA に関する詳細情報を表示します。

```
ciscoasa# show isis neighbors detail

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint        22.22.22.5        UP    23             c2.01
  Area Address(es): 49.0001
```

```
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
routerA          L2    subint        22.22.22.5        UP    22              c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
```

表 9-5　show isis neighbors のフィールド

フィールド	説明
System Id	エリア内のシステムを識別する 6 バイト値。
タイプ	レベルのタイプ。IS-IS ネイバーがレベル 1、レベル-1-2、またはレベル 2 のルータのいずれであるかを示します。
インターフェイス	システムが学習されたインターフェイス。
IP Address	ネイバー ルータの IP アドレス。
状態	IS-IS ネイバーの状態がアップかダウンか示します。
Holdtime	リンクステート パケット(LSP)のホールド時間。LSP が有効である時間(秒単位)。
Circuit Id	IS-IS 近接ルータがどのようにローカル ルータに接続されているかを示す、IS-IS 近接ルータのポート ロケーション。
Area Address(es)	ルータから到達可能なエリア アドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリア アドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリア アドレスになります。
SNPA	サブネットワーク ポイント オブ アタッチメント。これはデータ リンク アドレスです。
State Changed	状態が変化しました。
LAN Priority	LAN のプライオリティ。
Remote TID	近接ルータ トポロジの ID。
Local TID	ローカル ルータ トポロジの ID。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。

コマンド	説明
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis rib

特定のルートのパス、または IP ローカル ルーティング情報ベース（RIB）に格納されているメジャー ネットワーク下での全ルートのパスを表示するには、特権 EXEC モードで **show isis rib** コマンドを使用します。

show isis [* | **ip** [**unicast**] | **ipv6** [**unicast**]] **rib** [**redistribution** [**level-1** | **level-2**]] [*network_ip* [*mask*]]

構文の説明

*	（オプション）すべての IS-IS アドレス ファミリを表示します。
ip	（オプション）IPv4 アドレス ファミリを表示します。
ipv6	（オプション）IPv6 アドレス ファミリを表示します。
level-1	（オプション）レベル 1 再配布 RIB を表示します。
level-2	（オプション）レベル 2 再配布 RIB を表示します。
network_ip [***mask***]	（オプション）ネットワークの RIB 情報を表示します。
再配布	（オプション）IS-IS IP 再配布 RIB 情報を表示します。
unicast	（オプション）ユニキャスト アドレス ファミリを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

IP グローバル RIB 内に存在する IP プレフィックス アップデートが、IS-IS ローカル RIB 内で更新されたことを確認するには、**show isis rib** コマンドを入力します。

例

次に、IS-IS ローカル RIB 内に格納されたすべてのルートを表示する場合の **show isis rib** コマンドの出力例を示します。

```
ciscoasa# show isis rib

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =

10.10.0.0 255.255.0.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

次に、IS-IS ローカル RIB 内に格納されている、IP アドレスが 10.3.2.0 のメジャー ネットワーク 10.0.0.0 下の全ルータを表示する場合の **show isis rib** コマンドの出力例を示します。

```
ciscoasa# show isis rib 10.3.2.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =
Routes under majornet 10.0.0.0 255.0.0.0:

10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

次に、IS-IS ローカル RIB 内に格納されている、IP アドレス マスクが 10.3.2.0 255.255.255.0 のネットワーク下の全ルータを表示する場合の **show isis rib** コマンドの出力例を示します。

```
ciscoasa# show isis rib 10.3.2.0 255.255.255.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =

10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。

コマンド	説明
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis spf-log

ルータがフル最短パス優先(SPF)計算を実行した頻度と理由を表示するには、特権 EXEC モードで **show isis spf-log** コマンドを使用します。

show isis [* | **ip** [**unicast**] | **ipv6** [**unicast**]] **spf-log**

構文の説明

*	(オプション)すべての IS-IS アドレス ファミリを表示します。
ip	(オプション)IPv4 アドレス ファミリを表示します。
ipv6	(オプション)IPv6 アドレス ファミリを表示します。
unicast	(オプション)ユニキャスト アドレス ファミリを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ルータがフル最短パス優先(SPF)計算を実行した頻度と理由を表示します。

例

次に、**show isis ipv6 spf-log** コマンドの出力例を示します。

```
ciscoasa# show isis ipv6 spf-log

      TID 0 level 1 SPF log
  When   Duration  Nodes  Count     First trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
```

```
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

表 9-6　show isis spf-log のフィールド

フィールド	説明
When	今からどれくらい前(時間:分:秒)にフル SPF 計算が発生したか。直近 20 回分の発生内容が記録されます。
持続時間	今回の SPF 実行を完了させるために必要なミリ秒数。経過時間は実経過時間であり、CPU 時間ではありません。
ノード	今回の SPF 実行で計算されるトポロジを生成するルータおよび疑似ノード(LAN)の数。
Count	今回の SPF 実行をトリガーしたイベントの数。トポロジが変更されると、複数のリンクステート パケット(LSP)が短時間で受信されます。ルータは、フル SPF を実行するまでに 5 秒待機し、すべての新しい情報を保持できるようにします。この数は、ルータがフル SPF を実行するまで 5 秒待機する間に発生した(新しい LSP の受信のような)イベントの数を意味します。
First trigger LSP	新しい LSP の到着でフル SPF 計算がトリガーされると、常にルータは LSP ID を保存します。LSP ID は、エリア内でルーティングが不安定である原因の手掛かりを提供できます。複数の LSP が 1 つの SPF を実行すると、最後に受信された LSP の LSP ID だけが記憶されます。
Triggers	フル SPF 計算をトリガーしたすべての理由のリスト。トリガーに関する次の表を参照してください。

表 9-7　spf-log Triggers

Trigger	説明
ATTACHFLAG	このルータは、レベル 2 バックボーンに接続されるているか、または、レベル 2 バックボーンとの接続を失ったばかりです。
ADMINDIST	このルータの IS-IS プロセスに、別のアドミニストレーティブ ディスタンスが設定されました。
AREASET	このエリアの学習されたエリア アドレスの設定が変更されました。
BACKUPOVFL	IP プレフィックスが失われました。ルータはそのプレフィックスに到達するために別の方法があることを知っていますが、そのバックアップ ルートを保存していません。別のルートを見つける唯一の方法は、フル SPF の実行です。
DBCHANGED	このルータで、clear isis * コマンドが発行されました。

表 9-7　spf-log Triggers（続き）

Trigger	説明
IPBACKUP	IP ルートが失われましたが、これは IS-IS を介してではなく、優れたアドミニストレーティブ ディスタンスを持つ別のプロトコルを介して学習されました。IS-IS はフル SPF を実行し、失われた IP プレフィックスまでの IS-IS ルートをインストールします。
IPQUERY	このルータで、clear ip route コマンドが発行されました。
LSPEXPIRED	リンクステート データベース（LSDB）内のいくつかの LSP の期限が切れました。
LSPHEADER	LSP ヘッダー内の ATT/P/OL ビットまたは IS タイプが変更されました。
NEWADJ	このルータが、別のルータとの新しい隣接関係を作成しました。
NEWAREA	このルータに、新しいエリアが（Network Entity Title [NET] を介して）設定されました。
NEWLEVEL	このルータに、（IS タイプを介して）新しいレベルが設定されました。
NEWLSP	トポロジ内に新しいルータまたは疑似ノードが現れました。
NEWMETRIC	このルータのインターフェイスに、新しいメトリックが設定されました。
NEWSYSID	このルータに、（NET を介して）新しいシステム ID が設定されました。
PERIODIC	ルータは通常、15 秒ごとの間隔でフル SPF 計算を実行します。
RTCLEARED	このルータで、clear clns route コマンドが発行されました。
TLVCODE	TLV コードの不一致であり、最新バージョンの LSP に異なる TLV が含まれていることを示します。
TLVCONTENT	TLV のコンテンツが変更されました。これは通常、エリア内で隣接関係がアップまたはダウンしたこを示します。「First trigger LSP」カラムは、不安定な状態が発生した可能性のある場所を示します。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。

コマンド	説明
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。

コマンド	説明
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show isis topology

すべてのエリア内の接続された全ルータのリストを表示するには、特権 EXEC モードで **show isis topology** コマンドを使用します。

show isis [* | **ip** [**unicast**] | **ipv6** [**unicast**]] **topology** [**level-1** | **level-2**]

構文の説明

*	(オプション)すべての IS-IS アドレス ファミリを表示します。
ip	(オプション)IPv4 アドレス ファミリを表示します。
ipv6	(オプション)IPv6 アドレス ファミリを表示します。
level-1	(オプション)エリア内のすべてのレベル 1 ルータへのパスを表示します。
level-2	(オプション)ドメイン内のすべてのレベル 2 ルータへのパスを表示します。
unicast	(オプション)ユニキャスト アドレス ファミリを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

show isis topology コマンドを使用すると、すべてのエリア内の全ルータの存在およびルータ間の接続状態を確認できます。

例

次に、**show isis topology** コマンドの出力例を示します。

```
ciscoasa# show isis topology

IS-IS TID 0 paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                 --
routerA               10            routerA                subint       0025.8407.f2b0
```

```
c3                          10
c2                          10            c2                            subint
c08c.60e6.986f

IS-IS TID 0 paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA               10            routerA                 subint       0025.8407.f2b0
c3                          10
c2                          10            c2                           subint
c08c.60e6.986f
```

表 9-8　show isis topology のフィールド

フィールド	説明
System Id	エリア内のシステムを識別する 6 バイト値。
メトリック	送信側ルータとアドバタイズされたネイバー間の隣接関係のコスト用の IS-IS メトリック、またはアドバタイズ元のルータからアドバタイズ対象の宛先（IP アドレス、エンド システム [ES]、または CLNS プレフィックス）に到達するコスト用のメトリック。
Next-Hop	ネクスト ホップ ルータのアドレス。
インターフェイス	システムが学習されたインターフェイス。
SNPA	サブネットワーク ポイント オブ アタッチメント。これはデータ リンク アドレスです。

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。

コマンド	説明
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。

コマンド	説明
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

show kernel

デバッグに使用できる Linux brctl ユーティリティが提供する情報を表示するには、特権 EXEC モードで **show kernel** コマンドを使用します。

show kernel [process | bridge | cgroup-controller | ifconfig | module]

構文の説明

bridge	タップのブリッジを表示します。
cgroup-controller	cgroup-controller の統計情報を表示します。
ifconfig	タップおよびブリッジ インターフェイスの統計情報を表示します。
module	インストールおよび実行されているモジュールを表示します。
process	ASA で実行されているアクティブなカーネル プロセスの現在のステータスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.4(1)	**cgroup-controller** キーワードが追加されました。
8.6(1)	**ifconfig**、**module**、および **bridge** キーワードが追加されました。

使用上のガイドライン

このコマンドは、カーネルで実行されるさまざまなプロセスの統計情報を表示します。

例

次に、**show kernel process** コマンドの出力例を示します。

```
ciscoasa# show kernel process

PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
```

```
  5     1  20 -5           0         0 3725736671     S         0 kthread
  7     5  10 -5           0         0 3725736671     S         0 kblockd/0
  8     5  20 -5           0         0 3726794334     S         0 kseriod
 66     5  20  0           0         0 3725811768     S         0 pdflush
 67     5  15  0           0         0 3725811768     S         0 pdflush
 68     1  15  0           0         0 3725824451     S         2 kswapd0
 69     5  20 -5           0         0 3725736671     S         0 aio/0
171     1  16  0      991232        80 3725684979     S         0 init
172   171  19  0      983040       268 3725684979     S         0 rcS
201   172  21  0     1351680       344 3725712932     S         0 lina_monitor
202   201  16  0 1017602048    899932 3725716348     S       212 lina
203   202  16  0 1017602048    899932          0     S         0 lina
204   203  15  0 1017602048    899932          0     S         0 lina
205   203  15  0 1017602048    899932 3725712932     S         6 lina
206   203  25  0 1017602048    899932          0     R 13069390 lina
ciscoasa#
```

表 9-9 に、各フィールドの説明を示します。

表 9-9　　show kernel process のフィールド

フィールド	説明
PID	プロセス ID。
PPID	親プロセス ID。
PRI	プロセスのプライオリティ。
NI	プライオリティの計算に使用されるナイス値。値は 19（最大ナイス値）～ -19（最小ナイス値）の範囲です。
VSIZE	仮想メモリのサイズ（バイト単位）。
RSS	プロセスの Resident Set Size（KB 単位）。
WCHAN	プロセスが待機しているチャネル。
STAT	プロセスの状態。 • R：実行中 • S：割り込み可能な待機状態でスリープ中 • D：割り込み不可能なディスク スリープで待機中 • Z：ゾンビ • T：トレースまたは停止（信号による） • P：ページング
RUNTIME	プロセスがユーザ モードまたはカーネル モードでスケジュールされている jiffy の数。実行時間は utime と stime の合計です。
COMMAND	プロセス名。

次に、**show kernel module** コマンドの出力例を示します。

```
ciscoasa# show kernel module

Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
tscsync                 3852  0
```

次に、**show kernel ifconfig** コマンドの出力例を示します。

```
ciscoasa# show kernel ifconfig

br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)

br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)

tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)

tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)

tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

関連コマンド

コマンド	説明
show module	ASA にインストールされているモジュールに関する情報を表示します。

show kernel bridge

デバッグに使用できる各ポート上で学習された Linux ブリッジ、それらのメンバー ポート、および MAC アドレスを表示するには、特権 EXEC モードで **show kernel bridge** コマンドを使用します。

show kernel bridge [**mac-address** *bridge name*]

構文の説明

bridge name	ブリッジの名前を表示します。
mac-address	各ポートに関連付けられた MAC アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、デバッグに使用できる各ポート上で学習された Linux ブリッジ、それらのメンバー ポート、および MAC アドレス（リモート MAC アドレスを含む）を表示します。

例

次に、**show kernel bridge** コマンドの出力例を示します。

```
ciscoasa# show kernel bridge

bridge name    bridge id         STP enabled interfaces
br0         8000.0e3cd8a8909f    no         tap1
                                tap3
br1        8000.26d29f51a490     no         tap2
                                tap4
                                tap5hostname#
```

次に、**show kernel bridge mac-address** コマンドの出力例を示します。

```
ciscoasa# show kernel bridge mac-address br1

port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

関連コマンド

コマンド	説明
show kernel	ASA にインストールされているモジュールに関する情報を表示します。

show lacp

EtherChannel LACP 情報（トラフィック統計情報、システム ID、およびネイバーの詳細など）を表示するには、特権 EXEC モードで次のコマンドを入力します。

show lacp {[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}

構文の説明

channel_group_number	（オプション）EtherChannel チャネル グループ番号を 1 ～ 48 の範囲で指定して、このチャネル グループに関する情報だけを表示します。
counters	送受信された LACPDU 数およびマーカー数のカウンタを表示します。
internal	内部情報を表示します。
neighbor	ネイバー情報を表示します。
sys-id	LACP システム ID を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

例

次に、**show lacp sys-id** コマンドの出力例を示します。

```
ciscoasa# show lacp sys-id
32768,001c.c4e5.cfee
```

次に、**show lacp counters** コマンドの出力例を示します。

```
ciscoasa# show lacp counters

            LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv    Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 1
Gi3/1      736    728      0      0        0      0         0
Gi3/2      739    730      0      0        0      0         0
Gi3/3      739    732      0      0        0      0         0
```

次に、**show lacp internal** コマンドの出力例を示します。

```
ciscoasa# show lacp internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d
```

次に、**show lacp neighbor** コマンドの出力例を示します。

```
ciscoasa# show lacp neighbor

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

show lacp cluster

cLACP システムの MAC および ID を表示するには、特権 EXEC モードで **show lacp cluster** コマンドを使用します。

show lacp cluster {**system-mac** | **system-id**}

構文の説明

system-mac	システム ID と、それが自動生成されたのか手動入力されたのかを表示します。
system-id	システム ID およびプライオリティを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

clacp system-mac コマンドを使用して cLACP システムの ID およびプライオリティを設定します。

例

次に、**show lacp cluster system-mac** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

次に、**show lacp cluster system-id** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show lacp cluster system-id
5    ,a300.010a.010a
```

関連コマンド

コマンド	説明
clacp system-mac	cLACP システムの ID およびプライオリティを設定します。

show license

スマート ライセンスのステータスを表示するには、特権 EXEC モードで **show license** コマンドを使用します。

(注) この機能は、ASAv だけでサポートされています。

show license [all | entitlement | cert | pool | registration | features

構文の説明

all	スマート ライセンスの状態、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバル コンプライアンス ステータス、権限付与ステータス、ライセンス証明書情報、およびスマート エージェント タスクのスケジュールを表示します。
entitlement	使用中の各権限、ハンドル（整数 ID など）、数、タグ、強制モード（適合、非適合など）、バージョン、および権限が要求されたタイミングに関する詳細情報を表示します。
cert	ID 証明書の内容、発行日、および有効期限を表示します。
プール	このデバイスが割り当てられる権限付与プールを表示します。
登録	現在のスマート ライセンスの登録ステータスを表示します。
機能	現在のライセンスを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

show activation-key コマンドは、show license features コマンドと同じ出力を提供します。

例

次に、基本ライセンスのみ（現在のライセンス権限なし）の ASAv の例を示します。

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

show lisp eid

ASA EID テーブルを表示するには、特権 EXEC モードで **show lisp eid** コマンドを使用します。

show lisp eid [**site-id** *id*]

構文の説明

site-id *id*	特定のサイトの EID のみを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は EID とサイト ID を相関付ける EID テーブルを維持します。テーブルを表示するには、**show lisp eid** コマンドを使用します。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid** および **validate-key** コマンドを参照してください。

2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、**show lisp eid** コマンドの出力例を示します。

```
ciscoasa# show lisp eid
LISP EID       Site ID
10.44.33.105        2
10.44.33.201        2
192.168.11.1        4
192.168.11.2        4
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフロー モビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

show local-host

ローカル ホストのネットワーク状態を表示するには、特権 EXEC モードで **show local-host** を使用します。

show local-host [*hostname* | *ip_address*] [**detail**] [**brief**] [**all**] [**connection** {**sctp** | **tcp** | **udp** | **embryonic**} *start*[-*end*]] [**zone** [*zone-name*]]

構文の説明

all	(廃止)ASA に接続するローカルホストと、ASA から接続するローカルホストが含まれます。
brief	(オプション)ローカル ホストに関する簡潔な情報を表示します。
connection {**sctp** | **tcp** | **udp** | **embryonic**} *start*[-*end*]	(廃止)番号と接続のタイプに基づいて、初期、TCP、UDP、または SCTP のフィルタを適用します。*start* の数値は、そのタイプの最小接続数を示します。-*end* の数値を含めると、10-100 などの範囲を指定できます。これらのフィルタは個別に使用することも、組み合わせて使用することもできます。
detail	(任意)アクティブな xlate およびネットワーク接続の詳細情報を含めた、ローカル ホスト情報の詳細なネットワーク状態を表示します。
hostname | *ip_address*	(オプション)ローカル ホスト名または IPv4/IPv6 アドレスを指定します。
zone [*zone_name*]	(オプション)ゾーンごとにローカル ホストを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	ホスト制限があるモデルでは、このコマンドにより、外部インターフェイスと見なされるインターフェイスが表示されるようになりました。
7.2(4)	新しい 2 つのオプション、**connection** と **brief** が **show local-host** コマンドに追加され、出力が内部ホストの接続数でフィルタリングされるようになりました。
9.1(2)	テレメトリ ベースのアラートとしてシスコに Smart Call Home 情報を送信するコマンドが、**show local-host** コマンドから **show local-host | include interface** コマンドに変更されました。これは、インターフェイス アドレス情報を提供します。

リリース	変更内容
9.3(2)	**zone** キーワードが追加されました。
9.5(2)	表示が変更され、アスタリスク (*) でバックアップ ポートのブロックが示されるようになりました。
9.5(2)	SCTP 接続が出力に追加されました。**connection sctp** キーワードが追加されました。
9.14(1)	接続フィルタのキーワード: 初期、TCP、UDP、または SCTP は廃止されました。

使用上のガイドライン

show local-host コマンドを使用すると、ローカル ホストのネットワーク状態を表示できます。ローカル ホストは、トラフィックを ASA に送信するか、またはトラフィックを通じて転送する任意のホストに対して作成されます。

このコマンドを使用すると、ローカル ホストの変換スロットおよび接続スロットを表示できます。変換情報には、ホストに割り当てられた PAT ポートのブロックが含まれます。

ホスト制限のあるモデルの場合、ルーテッド モードで、内部のホスト(ワーク ゾーンとホーム ゾーン)は、外部(インターネット ゾーン)と通信するときにのみ制限値にカウントされます。インターネット ホストは制限値にカウントされません。ワークとホームの間のトラフィックを開始するホストも、制限値にカウントされません。デフォルト ルートに関連付けられたインターフェイスは、インターネット インターフェイスと見なされます。デフォルト ルートがない場合、すべてのインターフェイス上のホストが制限値にカウントされます。トランスペアレント モードでは、ホスト数が最小のインターフェイスがホスト制限値にカウントされます。

廃止されたオプション

このコマンドでは、接続の制限数も表示されます。接続制限が設定されていない場合、値として 0 が表示され、制限は適用されません。

TCP 代行受信が設定されている場合に、SYN 攻撃が発生すると、**show local-host** コマンド出力では、代行受信された接続の数が使用回数に計上されます。このフィールドは通常、完全なオープン接続のみを表示します。

show local-host コマンド出力では、スタティック接続を使用するホストに対して最大初期接続の制限値(TCP 代行受信の水準点)が設定されている場合に、**TCP embryonic count to host counter** が使用されます。このカウンタは、他のホストからこのホストに向かう初期接続の合計を示します。この合計が設定された最大制限値を超過すると、このホストへの新規接続に TCP 代行受信が適用されます。

例

次に、**show local-host** コマンドの出力例を示します。

```
ciscoasa# show local-host

Interface mgmt: 2 active, 2 maximum active
local host: <10.24.250.191>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 1
```

```
    TCP intercept watermark = unlimited
    UDP flow count/limit = 5/unlimited
Interface inside: 0 active, 0 maximum active,
Interface outside: 0 active, 0 maximum active
Interface any: 0 active, 0 maximum active, 0 denied
```

次に、ホスト制限がある ASA での **show local-host** コマンドの出力例を示します。

```
ciscoasa# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all other
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

次に、ホスト制限がある ASA での **show local-host** コマンドの出力例を示します。ただし、デフォルト ルートがない場合、ホスト制限はすべてのインターフェイスに適用されます。デフォルト ルート インターフェイスは、デフォルト ルートまたはルートが使用するインターフェイスがダウンしている場合は検出できないことがあります。

```
ciscoasa# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface c1in: 1 active, 1 maximum active
Interface c1out: 0 active, 0 maximum active
```

次に、ホスト制限がない ASA での **show local-host** コマンドの出力例を示します。

```
ciscoasa# show local-host
Licensed host limit: Unlimited

Interface c1in: 1 active, 1 maximum active
Interface c1out: 0 active, 0 maximum active
```

次の例では、特定のホストに関する情報に続けて、そのホストの詳細情報を示しています。

```
ciscoasa# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active
Interface inside: 1 active, 1 maximum active
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active

ciscoasa# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active
Interface inside: 1 active, 1 maximum active
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
```

```
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active,
1 maximum active
```

関連コマンド

コマンド	説明
clear local-host	(廃止)**show local-host** コマンドによって表示されるローカルホストからのネットワーク接続を解放します。
nat	ネットワークをグローバル IP アドレス プールに関連付けます。

show logging

バッファ内のログまたはその他のロギング設定を表示するには、特権 EXEC モードで **show logging** コマンドを使用します。

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting** | **flow-export-syslogs**]

構文の説明

all	（任意）すべての syslog メッセージ ID と、有効か無効かを表示します。
asdm	（任意）ASDM ロギング バッファの内容を表示します。
flow-export-syslogs	（オプション）NetFlow に送信されるメッセージと、それらがイネーブルかディセーブルかを表示します。
message	（任意）デフォルト以外のレベルにあるメッセージを表示します。メッセージ レベルを設定するには、**logging message** コマンドを参照してください。
queue	（任意）syslog メッセージ キューを表示します。
設定	（任意）ロギング設定を表示します。ロギング バッファは表示されません。
syslog_id	（任意）表示するメッセージ番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	syslog サーバが SSL/TLS 接続を使用するように設定されているかどうかを示します。
8.1(1)	**flow-export-syslogs** キーワードが追加されました。
8.4(1)	**show logging** コマンドでは、監査ブロックの現在の状態に関するエントリが出力に含まれます。
9.7(1)	このコマンドの出力には、IPv6 アドレスで設定された syslog サーバが含まれています。

使用上のガイドライン

logging buffered コマンドを使用している場合、キーワードなしの **show logging** コマンドからは、現在のメッセージ バッファと現在の設定が表示されます。

show logging queue コマンドを使用すると、次の情報を表示できます。

- キュー内のメッセージ数
- キュー内に記録されたメッセージの最大数
- 処理に利用できるブロック メモリがなかったために廃棄されたメッセージ数
- トラップおよび他の syslog メッセージごとに別々のキュー

(注) ゼロは、設定するキュー サイズとして許容される数値であり、最大許容キュー サイズを示します。設定されたキュー サイズが 0 の場合は、**show logging queue** コマンドの出力に実際のキュー サイズが示されます。

例

次に、**show logging** コマンドの出力例を示します。

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging:disabled
    Debug-trace logging: disabled
    Console logging: level informational, 3962 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 20549 messages logged
        Logging to inside 10.2.5.3 tcp/50001 connected
    Permit-hostdown state
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

(注) *state* の有効な値は、enabled、disabled、disabled-blocking、および disabled-not blocking です。

次に、セキュア syslog サーバが設定された **show logging** コマンドの出力例を示します。

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
ciscoasa(config)# show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

次に、**show logging queue** コマンドの出力例を示します。

```
ciscoasa(config)# show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

次に、**show logging message all** コマンドの出力例を示します。

```
ciscoasa(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

次に、NetFlow に送信されるメッセージと、それらがイネーブルかディセーブルかを表示する例を示します。

```
ciscoasa# show logging flow-export-syslogs
Syslog ID       Type                            Status
302013          Flow Created                    Enabled
302015          Flow Created                    Enabled
302017          Flow Created                    Enabled
302020          Flow Created                    Enabled
302014          Flow Deleted                    Enabled
302016          Flow Deleted                    Enabled
302018          Flow Deleted                    Enabled
302021          Flow Deleted                    Enabled
106015          Flow Denied                     Enabled
106023          Flow Denied                     Enabled
313001          Flow Denied                     Enabled
313008          Flow Denied                     Enabled
710003          Flow Denied                     Enabled
106100          Flow Created/Denied             Enabled
```

関連コマンド

コマンド	説明
logging asdm	ASDM へのロギングをイネーブルにします。
logging buffered	バッファへのロギングをイネーブルにします。
logging flow-export-syslogs	NetFlow データに関連付けられている syslog メッセージをイネーブルまたはディセーブルにします。
logging host	syslog サーバを定義します。
logging message	メッセージ レベルを設定するか、またはメッセージをディセーブルにします。
logging queue	ロギング キューを設定します。

show mac-address-table

MAC アドレス テーブルを表示するには、特権 EXEC モードで **show mac-address-table** コマンドを使用します。

show mac-address-table [*interface_name* | **count** | **static** | **vtep-mapping**]

構文の説明

count	(任意)ダイナミックおよびスタティック エントリの合計数を一覧します。
interface_name	(任意)MAC アドレス テーブル エントリを表示するインターフェイス名を指定します。
静的	(任意)スタティック エントリのみを一覧します。
vtep-mapping	(オプション)リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。

デフォルト

インターフェイスを指定しない場合、すべてのインターフェイス MAC アドレス エントリが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.4(1)	**vtep-mapping** キーワードが追加されました。
9.7(1)	ルーテッド モードのサポートが追加されました。

例

次に、**show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table
interface          mac address       type      Time Left
------------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

次に、内部インターフェイスの **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table inside
interface          mac address       type      Time Left
------------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

次に、**show mac-address-table count** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

show mac-address-table vtep-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show mac-address-table vtep-mapping
interface                   mac  address       type    Age(min)   bridge-group    VTEP
------------------------------------------------------------------------------------------------
------
vni-outside                00ff.9200.0000      dynamic      5          1      10.9.1.3
vni-inside                 0041.9f00.0000      dynamic      5          1      10.9.1.3
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。

show mac-learn

各インターフェイスに対して MAC ラーニングがイネーブルかディセーブルかを表示するには、特権 EXEC モードで **show mac-learn** を使用します。

show mac-learn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	ルーテッド モードのサポートが追加されました。

使用上のガイドライン

デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、システムは対応するエントリを MAC アドレス テーブルに追加します。インターフェイスごとに MAC ラーニングをディセーブルにすることができます。

例

次に、**show mac-learn** コマンドの出力例を示します。

```
ciscoasa# show mac-learn
no mac-learn flood
interface                           mac learn
-----------------------------------------
 outside                              enabled
 inside1_2                            enabled
 inside1_3                            enabled
 inside1_4                            enabled
 inside1_5                            enabled
 inside1_6                            enabled
 inside1_7                            enabled
 inside1_8                            enabled
 diagnostic                           enabled
 inside                               enabled
```

関連コマンド

コマンド	説明
mac-learn	MAC アドレス ラーニングをディセーブルにします。

show management-access

管理アクセスに設定された内部インターフェイスの名前を表示するには、特権 EXEC モードで show management-access コマンドを使用します。

show management-access

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます(インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 " " に囲まれて表示されます)。

例

次に、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定し、結果を表示する例を示します。

```
ciscoasa(config)# management-access inside
ciscoasa(config)# show management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	ASA の管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
management-access	管理アクセス用の内部インターフェイスを設定します。

show-map-domain

マッピングアドレスおよびポート(MAP)ドメインを表示するには、特権 EXEC モードで **show map-domain** コマンドを使用します。

show map-domain

デフォルト

デフォルト設定はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォールモード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード。	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが導入されました。

使用上のガイドライン

show map-domain コマンドによって MAP コンフィギュレーションが表示されます(**show running-config map-domain** と同様)が、同時にドメイン設定が有効かどうかも示されます。

例

次の例には、2 つのドメイン(1 と 2)があります。この出力では、MAP ドメイン 2 が不完全なためにアクティブではないことが説明されています。

```
ciscoasa(config)# show map-domain

MAP Domain 1
  Default Mapping Rule
    IPv6 prefix 2001:db8:cafe:cafe::/64
  Basic Mapping Rule
    IPv6 prefix 2001:cafe:cafe:1::/64
    IPv4 prefix 192.168.3.0 255.255.255.0
    share ratio 16
    start port 1024
    PSID length 4
    PSID offset 6
    Rule EA-bit length 12

MAP Domain 2
  Default Mapping Rule
    IPv6 prefix 2001:db8:1234:1234::/64

Warning: map-domain 2 configuration is incomplete and not in effect.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート(MAP)ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート(MAP)ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

show memory

物理メモリの最大量、およびオペレーティング システムで現在使用可能な空きメモリ量の要約を表示するには、特権 EXEC モードで **show memory** コマンドを使用します。

show memory [**detail**]

構文の説明

detail	（任意）空きメモリおよび割り当て済みシステム メモリの詳細ビューを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.2(1)	ASAv をサポートするために、仮想マシン（VM）の統計情報が出力に追加されました。
9.3(2)	内部メモリ マネージャが **show memory detail** コマンドの標準 glibc ライブラリに置き換えられました。

使用上のガイドライン

show memory コマンドで、物理メモリの最大量およびオペレーティング システムで現在使用可能な空きメモリ量の要約を表示できます。メモリは必要に応じて割り当てられます。

SNMP を使用して **show memory** コマンドから情報を表示することもできます。

show memory detail の出力を **show memory binsize** コマンドとともに使用して、メモリ リークをデバッグできます。

show memory detail コマンド出力は、要約、DMA メモリ、ヒープ メモリの 3 つのセクションに分割できます。要約には、メモリ全体の割り当てが表示されます。DMA にリンクしていないメモリ、または予約されていないメモリは、ヒープと見なされます。Free memory の値は、ヒープ内の未使用メモリです。Used memory の値は、割り当て済みのメモリの合計を示します。ヒープ割り当ての明細は、出力の後半で表示されます。予約メモリおよび DMA 予約メモリは、別のシステム プロセスおよび主に VPN サービスによって使用されます。

Free memory は、Heapcache Pool、Global Shared Pool、および System の 3 つの部分に分かれています。Heapcache Pool と Global Shared Pool は、glibc ヒープで利用可能なメモリの空き容量です。System は、基盤となるシステムから割り当てることができる使用可能なメモリです。ASA で使用可能な Free memory の総容量は、Heapcache Pool、Global Shared Pool、および System の合計です。

Used memory は Heapcache Pool、Global Shared Pool、Reserved、および System Overhead の 4 つの部分に分かれています。Heapcache Pool と Global Shared Pool プールは、glibc ヒープの Used memory の容量です。予約メモリ（DMA）は、DMA のプールに予約されているメモリ量です。System オーバーヘッドは、さまざまな実行プロセスの glibc オーバーヘッドおよびプロセス オーバーヘッドです。

- メモリは、起動時に DMA とヒープキャッシュ用に予約されます。
- 最初に、ヒープ メモリはヒープキャッシュから割り当てられ、その後にヒープキャッシュがなくなると、グローバル共有プールから割り当てられます。
- グローバル共有プールでは、必要に応じてシステムからメモリが渡されます。メモリが解放されて返せるようになるたびに、システムに返します。
- 空きヒープ メモリの合計は、ヒープキャッシュとグローバル共有プールのメモリ容量に、システムの空きメモリ容量を加えたものです。

割り当てられたメモリの統計情報の合計（バイト）列に表示される値は、**show memory detail** コマンド出力の実際の値（MEMPOOL_GLOBAL_SHARED POOL STATS）ではありません。

（注） バージョン 9.3(2) より前は、すべてのシステム メモリ（DMA プール用を除き）が MEMPOOL_GLOBAL_SHARED の一部として表示されます。つまり、すべての割り当て可能な空きメモリが、MEMPOOL_GLOBAL_SHARED にありました。バージョン 9.3(2) では、MEMPOOL_GLOBAL_SHARED は、ブートアップ時にすべてのシステム メモリを取得しませんが、必要なときは常に、基盤となるオペレーティング システムにメモリを要求します。同様に、大量のメモリが解放されたときは、システムにメモリが返されます。その結果、MEMPOOL_GLOBAL_SHARED のサイズは需要に応じて増減されて表示されます。割り当てを高速化するため、最小空きメモリ量は、MEMPOOL_GLOBAL_SHARED に残されます。

出力は、サイズ 49,152 のブロックが空きプールに割り当てられてから戻され、別のサイズ 131,072 のブロックが割り当てられていることを示します。この場合、空きメモリは 131,072-49,152=81,920 バイト単位で減少しますが、実際は 100,000 バイトずつ減少します（空きメモリの行を参照）。

```
ciscoasa# show memory detail

Free memory heap:                 1193358928 bytes (13%)
Free memory system:               6596267951 bytes (74%)
Used memory:
     Allocated memory in use:      464188448 bytes ( 5%)
     Reserved memory (DMA):        513802240 bytes ( 6%)
     Memory overhead:              202659216 bytes ( 2%)
-----------------------------   ------------------
Total memory:                     8970276783 bytes (100%)

Least free memory:       7963442431 bytes (89%)
Most used memory:        1006834352 bytes (11%)
MEMPOOL_HEAPCACHE_0 POOL STATS:

Non-mmapped bytes allocated =   1541406720
Number of free chunks       =          633
Number of mmapped regions   =            0
```

```
Mmapped bytes allocated     =            0
Max memory footprint        =   1541406720
Keepcost                    =   1190961440
Max contiguous free mem     =   1190961440
Allocated memory in use     =    348047792
Free memory                 =   1193358928

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           32           177           5664
           48           204           9792
           64           161          10304
           80             3            240
           96             1             96**
          112             2            224
          160             5            800
          192             1            192
          208             1            208
          224             1            224
          240             1            240
          256            13           4064
          384             2            864
          512             3           1648
         1024             1           1296
        12288             1          13792
        24576             2          57424
        32768             1          43824
        65536             1          65616
       262144             1         322672
      1572864             1        1843712
   1190961440             1     1190961440*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           80          1637         130960
           96         13898        1334208
          112          3422         383264
          128          1910         244480
          144          3677         529488
          160           463          74080
          176           856         150656
          192           357          68544
          208           350          72800
          224           370          82880
          240           337          80880
          256          2293         587008
          384           596         228864
          512           657         336384
          768           504         387072
         1024           449         459776
         1536          1217        1869312
         2048           376         770048
         3072           137         420864
         4096           652        2670592
```

```
         6144            73         448512
         8192           212        1736704
        12288           643        7901184
        16384           598        9797632
        24576            31         761856
        32768            77        2523136
        49152            31        1523712
        65536           200       13107200
        98304            30        2949120
       131072            20        2621440
       196608            28        5505024
       262144            14        3670016
       393216            23        9043968
       524288             5        2621440
       786432             9        7077888
      1048576            11       11534336
      1572864            10       15728640
      2097152             5       10485760
      3145728             3        9437184
      4194304             3       12582912
      6291456             1        6291456
      8388608             1        8388608
     12582912             7       88080384

MEMPOOL_DMA POOL STATS:

Non-mmapped bytes allocated =    513802240
Number of free chunks       =          153
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    513802240
Keepcost                    =    190724944
Max contiguous free mem     =    190724944
Allocated memory in use     =    322994736
Free memory                 =    190807504

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           48            30            1440
           96             1              96**
          112            28            3136
          160             1             160
          208             1             208
          224             1             224
          240             2             480
          256             1             288
          384            19            9104
          512            65           40656
          768             1             800
         1024             2            2608
    190724944             1       190724944*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
```

```
          160             1            160
          240            92          22080
          256             2            512
          512             2           1024
         1024           163         166912
         2048             5          10240
         8192             1           8192
        12288            18         221184
        16384             1          16384
        32768            38        1245184
        49152             1          49152
        65536             1          65536
       131072             4         524288
       196608             3         589824
       262144             8        2097152
       393216             6        2359296
       524288             2        1048576
       786432             1         786432
      1048576            11       11534336
      1572864             7       11010048
      3145728             8       25165824
      6291456             5       31457280
      8388608             1        8388608
     12582912             7       88080384

MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =       135168
Number of free chunks       =            4
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =            0
Keepcost                    =        51616
Max contiguous free mem     =        51616
Allocated memory in use     =         4064
Free memory                 =       131104

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
          432             1            432
        40960             1          50848

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           96             1             96
          112             1            112
          160             1            160
          208             3            624

Summary for all pools:

Non-mmapped bytes allocated =   2055344128
Number of free chunks       =          790
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =   2055208960
Keepcost                    =   1381738000
```

```
Allocated memory in use     =    671046592
Free memory                 =   1384297536
```

次の出力では、131,072 の代わりにサイズ 149,0327 のブロックが割り当てられたことを確認します。

```
ciscoasa# show memory binsize 131072
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7f739a97db9f, size = 1490327  , count = 9
pc = 0x7f7399be30a0, size = 309008   , count = 2
pc = 0x7f7399be31f4, size = 1255704  , count = 9
MEMPOOL_DMA pool bin stats:
pc = 0x7f73984ba38d, size = 323486   , count = 2
pc = 0x7f73984b8e55, size = 320286   , count = 2
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

show memory detail コマンドの出力に合計バイト数の概算が示されるのは仕様によるものです。これには次の 2 つの理由があります。

- 各フラグメント サイズに対して、すべてのフラグメントの合計を取得する必要があると、単一のフラグメント サイズの割り当て数が非常に多くなることで、パフォーマンスに影響する可能性があり、かつ、正確な値を取得するには、数千ものチャンクを実行することが必要になります。
- 各 binsize に対して、二重にリンクされた割り当てリスト全体を確認する必要があり、割り当ては多数存在する可能性があります。この場合、CPU を長期間占有できないため、割り当てを定期的に停止する必要があります。割り当てを再開した後、他のプロセスがメモリを割り当てまたは割り当て解除したことによって、メモリ状態が変化している可能性があります。このため、合計バイト列には、実際の値ではなく近似値が示されます。

例

次に、**show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
-------------     ------------------
Total memory:       4455811482 bytes (100%)
```

注：Free memory は、システムの空きメモリです。さらに、ASA プロセス内部のメモリ プールで使用可能なメモリを追加できる可能性があります。この情報を表示するには、show memory detail コマンドを使用します。ただし、CPU の占有や、ロード時のパケット損失が発生する可能性があるため慎重に使用してください。

次に、**show memory detail** コマンドの出力例を示します。

```
ciscoasa# show memory detail
Heap Memory:
   Free Memory:
      Heapcache Pool:                    447109376 bytes ( 10% )
      Global Shared Pool:                   131152 bytes (  0% )
      System:                           3208100250 bytes ( 72% )
   Used Memory:
      Heapcache Pool:                    257533696 bytes (  6% )
      Global Shared Pool:                     4016 bytes (  0% )
      Reserved (Size of DMA Pool):       234881024 bytes (  5% )
      System Overhead:                   308051968 bytes (  7% )
-------------------------------------    ----------------
   Total Memory:                        4455811482 bytes ( 100% )
```

```
Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.

------------------------------------------------------------------------
MEMPOOL_HEAPCACHE_0 POOL STATS:

Non-mmapped bytes allocated =    704643072
Number of free chunks       =          309
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    704643072
Keepcost                    =    446723584
Max contiguous free mem     =    446723584
Allocated memory in use     =    257533696
Free memory                 =    447109376

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           32           91          2912
           48          116          5568
           64           83          5312
           96            1            96**
           96            3           288
          112            1           112
          160            2           320
          224            2           448
          240            1           240
          256            2           544
          384            1           384
          512            2          1392
          768            2          1904
        32768            1         44704
    446723584            1     446723584*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           80          937          74960
           96        10758        1032768
          112         2051         229712
          128          898         114944
          144         2887         415728
          160          290          46400
          176          300          52800
          192          164          31488
          208          246          51168
          224          183          40992
          240          208          49920
          256         1396         357376
          384          474         182016
          512          305         156160
          768          322         247296
         1024          240         245760
         1536          321         493056
         2048          171         350208
```

```
         3072            45         138240
         4096           259        1060864
         6144            47         288768
         8192           174        1425408
        12288            94        1155072
        16384           571        9355264
        24576            17         417792
        32768            51        1671168
        49152            16         786432
        65536           121        7929856
        98304            14        1376256
       131072             9        1179648
       196608            19        3735552
       262144            12        3145728
       393216            15        5898240
       524288             2        1048576
       786432             9        7077888
      1048576            12       12582912
      1572864             5        7864320
      2097152             3        6291456
      3145728             2        6291456
      4194304             4       16777216
      6291456             3       18874368
      8388608             1        8388608
     12582912             3       37748736

MEMPOOL_DMA POOL STATS:

Non-mmapped bytes allocated =    234881024
Number of free chunks       =          162
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    234881024
Keepcost                    =     90103152
Max contiguous free mem     =     90103152
Allocated memory in use     =    144701888
Free memory                 =     90179136

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           96             1            96**
          112             1           112
          256            64         20480
          384            32         15360
          512            64         39936
     90103152             1       90103152*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
          160             2           320
          256             2           512
          512             1           512
         1024           160        163840
         2048             5         10240
```

```
         8192             1           8192
        12288            18         221184
        16384             1          16384
        32768            37        1212416
        49152             2          98304
        65536             1          65536
       131072             4         524288
       196608             2         393216
       262144             4        1048576
       393216             2         786432
       524288             2        1048576
       786432             1         786432
      1048576             3        3145728
      1572864             2        3145728
      3145728             3        9437184
      6291456             2       12582912
     12582912             3       37748736

MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =       135168
Number of free chunks       =            4
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =            0
Keepcost                    =        96368
Max contiguous free mem     =        96368
Allocated memory in use     =         4016
Free memory                 =       131152

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
          448             1            448
        20480             1          23296

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           96             1             96
          112             1            112
          160             1            160
          192             3            576

Summary for all pools:

Non-mmapped bytes allocated =    939659264
Number of free chunks       =          475
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    939524096
Keepcost                    =    536923104
Allocated memory in use     =    402239600
Free memory                 =    537419664

On 5585:
========

ciscoasa# show memory
Free memory:        4544618496 bytes (73%)
```

```
Used memory:        1714343936 bytes (27%)
-------------     ------------------
Total memory:       6258962432 bytes (100%)

Note: Free memory is the free system memory. Additional memory may
      be available from memory pools internal to the ASA process.
      Use 'show memory detail' to see this information, but use it
      with care since it may cause CPU hogs and packet loss under load.

ciscoasa# show memory detail

Heap Memory:
   Free Memory:
      Global Shared Pool:                  283589104 bytes (  5% )
      System:                             4544618496 bytes ( 73% )
   Used Memory:
      Global Shared Pool:                   41813520 bytes (  1% )
      Reserved (Size of DMA Pool):         445095936 bytes (  7% )
      System Overhead:                     943845376 bytes ( 15% )
-------------------------------------     ----------------
   Total Memory:                          6258962432 bytes ( 100% )

Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.

------------------------------------------------------------------------
MEMPOOL_DMA POOL STATS:

Non-mmapped bytes allocated =    445095936
Number of free chunks       =          161
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    445095936
Keepcost                    =    250149264
Max contiguous free mem     =    250149264
Allocated memory in use     =    194871536
Free memory                 =    250224400

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           64             1             64
           96             1             96**
          112             1            112
          256            63          20192
          384            32          15360
          512            63          39312
    250149264             1      250149264*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           80             1             80
          144             1            144
          160             2            320
          256             2            512
```

```
          512             1            512
         1024           160         163840
         2048             5          10240
         8192             5          40960
        12288            27         331776
        16384             1          16384
        32768            39        1277952
        49152             1          49152
        65536             1          65536
        98304             4         393216
       131072             4         524288
       196608             1         196608
       262144             3         786432
       393216             2         786432
       524288             2        1048576
       786432             5        3932160
      1048576             3        3145728
      1572864             2        3145728
      3145728             4       12582912
     12582912             4       50331648

MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =     43286528
Number of free chunks       =          474
Number of mmapped regions   =          156
Mmapped bytes allocated     =    282116096
Max memory footprint        =            0
Keepcost                    =        11200
Max contiguous free mem     =       132816
Allocated memory in use     =     41813520
Free memory                 =      1473008

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           32          135           4320
           48          203           9744
           64           38           2432
           80            2            160
           80           20           1600
           96            3            288
           96            3            288
          112           90          10080
          112           10           1120
          128           20           2560
          144            1            144
          240            1            240
          384            1            384
          400            1            400
          448            1            448
          480            1            480
          544            1            544
          560            6           3360
          656            1            656
          816            1            816
          832            1            832
          880            1            880
         1088            3           3360
         1664            1           1680
         3136            1           3280
         3584            1           3776
```

```
         8704             1           8704
        24576             1          25728
        40960             1          50064

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
           64           354          22656
           80          1234          98720
           96         12337        1184352
          112          1202         134624
          128           970         124160
          144          2777         399888
          160           435          69600
          176           155          27280
          192           323          62016
          208           250          52000
          224            86          19264
          240           388          93120
          256          1478         378368
          384           304         116736
          512           304         155648
          768           314         241152
         1024           410         419840
         1536          1188        1824768
         2048           136         278528
         3072            42         129024
         4096           814        3334144
         6144            56         344064
         8192           174        1425408
        12288           123        1511424
        16384           584        9568256
        24576            30         737280
        32768            60        1966080
        49152            30        1474560
        65536           139        9109504
        98304            25        2457600
       131072            19        2490368
       196608            32        6291456
       262144            18        4718592
       393216            29       11403264
       524288             7        3670016
       786432             8        6291456
      1048576            13       13631488
      1572864            11       17301504
      2097152             6       12582912
      3145728             2        6291456
      4194304             4       16777216
      8388608             1        8388608
     12582912             6       75497472

Summary for all pools:

Non-mmapped bytes allocated =    488382464
Number of free chunks       =          635
Number of mmapped regions   =            0
Mmapped bytes allocated     =    282116096
Max memory footprint        =    445095936
Keepcost                    =    250160464
Allocated memory in use     =    236685056
Free memory                 =    251697408
```

次に、**jumbo-frame reservation** コマンドをイネーブルにして **write memory** コマンドと **reload** コマンドを発行した後の、ASA 5525 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
-------------     ------------------
Total memory:       4455811482 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにしない ASA 5525 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
-------------     ------------------
Total memory:       4455811482 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにした後の、ASA 5515 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:        3276619472 bytes (76%)
Used memory:        1018347824 bytes (24%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにしない ASA 5515 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:        3481145472 bytes (81%)
Used memory:         813821824 bytes (19%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにした後の、ASA 5585 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:        8883297824 bytes (69%)
Used memory:        4001604064 bytes (31%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

次に、**jumbo-frame reservation** コマンドをイネーブルにしない ASA 5585 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:        9872205104 bytes (77%)
Used memory:        3012696784 bytes (23%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

次に、**jumbo-frame** コマンドをサポートしていない ASA 5520 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
ree memory:         206128232 bytes (38%)
Used memory:         330742680 bytes (62%)
-------------       -----------------
Total memory:        536870912 bytes (100%)
```

次に、**jumbo-frame** コマンドをサポートしていない ASA 5505 での **show memory** コマンドの出力例を示します。

```
ciscoasa# show memory
Free memory:           48457848 bytes (18%)
Used memory:          219977608 bytes (82%)
-------------         -----------------
Total memory:         268435456 bytes (100%
```

次に、ASAv での **show memory** コマンドの出力例を示します。

```
Free memory:         2694133440 bytes (63%)
Used memory:         1600833856 bytes (37%)
-------------      ------------------
Total memory:        4294967296 bytes (100%)

Virtual platform memory
-----------------------
Provisioned       4096 MB
Allowed           4096 MB
Status            Compliant
```

関連コマンド

コマンド	説明
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory api

システムに登録されている malloc スタック API を表示するには、特権 EXEC モードで **show memory api** コマンドを使用します。

show memory api

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、システムに登録されている malloc スタック API を表示します。

メモリ デバッグ機能（つまり、delay-free-poisoner、メモリ トラッカー、またはメモリ プロファイラ）がオンになっている場合、API が **show memory api** の出力に表示されます。

例

次に、**show memory api** コマンドの出力例を示します。

```
ciscoasa# show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

関連コマンド

コマンド	説明
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory app-cache

アプリケーションによるメモリ使用状況を確認するには、特権 EXEC モードで **show memory app-cache** コマンドを使用します。

show memory app-cache [**threat-detection** | **host** | **flow** | **tcb** | **http** | **access-list** | **tcb-ibs**] [**detail**]

構文の説明show

access-list	(オプション)アクセス リストのアプリケーション レベル メモリ キャッシュを表示します。
detail	(任意)空きメモリおよび割り当て済みシステム メモリの詳細ビューを表示します。
flow	(オプション)フローのアプリケーション レベル メモリ キャッシュを表示します。
ホスト	(オプション)ホストのアプリケーション レベル メモリ キャッシュを表示します。
http	(オプション)HTTP のアプリケーション レベル メモリ キャッシュを表示します。
tcb	(オプション)TCB のアプリケーション レベル メモリ キャッシュを表示します。
tcb-ips	(オプション)TCB-IPS のアプリケーション レベル メモリ キャッシュを表示します。
threat-detection	(オプション)脅威検出のアプリケーション レベル メモリ キャッシュを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(1)	このコマンドが追加されました。
8.1(1)	**access-list** および **http** オプションが追加されました。
9.10(1)	**tcb-ips** オプションが追加されました。

使用上のガイドライン

このコマンドを使用して、アプリケーションによるメモリ使用状況を確認できます。

例

次に、**show memory app-cache threat-detection** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache threat-detection
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

次に、**show memory app-cache threat-detection detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache threat-detection detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
TD ACE stats 50 0 2 0 1936
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host stats 50 50 16120 0 116515360
TD Subnet stats 50 2 113 0 207016
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

次に、**show memory app-cache host detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache host detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Core 0 1000 1000 5116 0 961808
SNP Host Core 1 1000 1000 4968 0 933984
SNP Host Core 2 1000 1000 5413 0 1017644
SNP Host Core 3 1000 1000 4573 0 859724

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 20070 0 3773160
```

次に、**show memory app-cache flow detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache flow detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn Core 0 1000 1000 893 0 639388
SNP Conn Core 1 1000 948 980 0 701680
SNP Conn Core 2 1000 1000 1175 0 841300
SNP Conn Core 3 1000 1000 901 0 645116

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 3948 3949 0 2827484
```

次に、**show memory app-cache access-list detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache access-list detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
NP ACL log c Core 0 1000 0 1 0 68
NP ACL log c Core 1 1000 0 6 0 408
```

```
NP ACL log c Core 2 1000 0 19 0 1292
NP ACL log c Core 3 1000 0 0 0 0
NP ACL log f Core 0 1000 0 0 0 0
NP ACL log f Core 1 1000 0 0 0 0
NP ACL log f Core 2 1000 0 0 0 0
NP ACL log f Core 3 1000 0 0 0 0

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 26 0 1768
```

次に、**show memory app-cache http detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache http detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
Inspect HTTP Core 0 1000 0 0 0 0
Inspect HTTP Core 1 1000 0 0 0 0
Inspect HTTP Core 2 1000 0 0 0 0
Inspect HTTP Core 3 1000 0 0 0 0
HTTP Result Core 0 1000 0 0 0 0
HTTP Result Core 1 1000 0 0 0 0
HTTP Result Core 2 1000 0 0 0 0
HTTP Result Core 3 1000 0 0 0 0

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 0 0 0
```

次に、**show memory app-cache tcb detail** コマンドの出力例を示します。

```
ciscoasa(config)# show memory app-cache tcb detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB Core 0 1000 1000 968 0 197472
SNP TCB Core 1 1000 1000 694 0 141576
SNP TCB Core 2 1000 1000 1304 0 266016
SNP TCB Core 3 1000 1000 1034 0 210936

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 4000 0 816000
```

次に、**show memory app-cache tcb-ips detail** コマンドの出力例を示します。

```
ha-asa5512a(config)# show memory app-cache tcb-ips detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB IPS Core 00     625 0 0 0 0
LIMIT      COUNT      ALLOC     FAILED   BYTES USED
TOTAL         625          0 0 0            0

ha-asa5512a(config)# show memory app-cache
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
[...]
SNP TCB IPS Core 00 625 0 0 0 0
SNP TCB IPS Total 625 0 0 0 0

[...]

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 61972 149 188 0        50212
```

関連コマンド

コマンド	説明
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。

show memory appcache-threshold

memory appcache-threshold のステータスとヒット カウントを表示するには、特権 EXEC モードで **show memory appcache-threshold** コマンドを使用します。

show memory appcache-threshold

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

管理対象アプリケーションのヒット カウントとメモリ割り当てしきい値のステータスを表示するには、**show memory appcache-threshold** コマンドを使用します。

例

次に、管理対象アプリケーションの memory appcache threshold のステータスを表示する例を示します。

```
ciscoasa# show memory appcache-threshold
          CACHE NAME   STATUS      THRESHOLD     HIT COUNT
    SNP Conn Core 00   ENABLED            85             5

ciscoasa# show memory appcache-threshold
          CACHE NAME   STATUS      THRESHOLD     HIT COUNT
    SNP Conn Core 00   DISABLED           85             5
```

表 9-10　show memory appcache-threshold のフィールド

フィールド	説明
Cache Name	管理対象のアプリケーション キャッシュの名前。ASA 9.10.1 リリースでは、SNP Conn Core 00 アプリケーションのキャッシュ タイプのみが管理されます。
Status（ステータス）	このアプリケーション キャッシュ タイプの appcache-threshold 機能が有効か無効かを示します。
Threshold	このアプリケーション キャッシュ タイプのしきい値。たとえば、「85」はシステムメモリの 85% が使用されていることを意味します。
Hit Count	カウンタが最後にクリアされてからこのしきい値にヒットした回数。

関連コマンドl

コマンド	説明
memory appcache-threshold enable	特定のメモリしきい値に達した後のアプリケーション キャッシュの割り当てを制限するには、memory appcache-threshold を有効にします。
clear memory appcache-threshold	memory appcache-threshold のヒット カウントをクリアします。

show memory binsize

特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示するには、特権 EXEC モードで **show memory binsize** コマンドを使用します。

show memory binsize *size*

構文の説明

size	特定のバイナリ サイズのチャンク（メモリ ブロック）を表示します。バイナリ サイズは **show memory detail** コマンド出力の「fragment size」列から取得されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには使用上のガイドラインがありません。

例

次に、バイナリ サイズ 500 に割り当てられたチャンクについての要約情報を表示する例を示します。

```
ciscoasa# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

関連コマンド

コマンド	説明
show memory-caller address	ASA 上に設定されているアドレス範囲を表示します。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。

show memory caller-address

ASA で設定されたアドレス範囲を表示するには、特権 EXEC モードで **show memory caller-address** コマンドを使用します。

show memory caller-address

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

アドレス範囲を **show memory-caller address** コマンドで表示する前に、**memory caller-address** コマンドで設定する必要があります。

例

次に、**memory caller-address** コマンドでアドレス範囲を設定する方法、および **show memory-caller address** コマンドの出力結果の例を示します。

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08
ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

アドレス範囲が **show memory-caller address** コマンドを入力する前に設定されていなかった場合、アドレスは表示されません。

```
ciscoasa# show memory-caller address
Move down stack frame for the addresses:
```

関連コマンド

コマンド	説明
memory caller-address	発信元 PC のメモリ ブロックを設定します。

show memory delayed-free-poisoner

memory delayed-free-poisoner キューの使用状況の要約を表示するには、特権 EXEC モードで **show memory delayed-free-poisoner** コマンドを使用します。

show memory delayed-free-poisoner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear memory delayed-free-poisoner コマンドを使用して、キューおよび統計情報をクリアします。

例

次に、**show memory delayed-free-poisoner** コマンドの出力例を示します。

```
ciscoasa# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
         3335600:  memory held in queue
            6095:  current queue count
               0:  elements dequeued
               3:  frees ignored by size
            1530:  frees ignored by locking
              27:  successful validate runs
               0:  aborted validate runs
        01:09:36:  local time of last validate
```

表 9-11 に、**show memory delayed-free-poisoner** コマンド出力での重要なフィールドの説明を示します。

*表 9-11　**show memory delayed-free-poisoner** コマンド出力の説明*

フィールド	説明
memory held in queue	delayed free-memory poisoner ツール キューに保留されたメモリ。delayed free-memory poisoner ツールがイネーブルになっていない場合、このようなメモリは、通常、**show memory** 出力では「空き」容量になります。
current queue count	キューにある要素の数。
elements dequeued	キューから削除された要素の数。この数は、システム内の空きメモリだったメモリの大部分またはすべてが最終的にキューに保持されることになった場合に増加し始めます。
frees ignored by size	要求が小さすぎて必要なトラッキング情報を保持できなかったため、キューに配置されなかった解放要求の数。
frees ignored by locking	複数のアプリケーションがメモリを使用しているため、キューに配置されずに、ツールによって代行受信された解放要求の数。最後にメモリを解放してシステムに戻したアプリケーションが、このメモリ領域をキューに割り当てます。
successful validate runs	**clear memory delayed-free-poisoner** コマンドを使用して、モニタリングがイネーブルにされた後、またはクリアされた後で、キューの内容が（自動的に、または **memory delayed-free-poisoner validate** コマンドによって）検証された回数。
aborted validate runs	**clear memory delayed-free-poisoner** コマンドを使用して、モニタリングがイネーブルにされた後、またはクリアされた後で、複数のタスク（定期的な実行または CLI からの検証要求）が同時にキューを使用しようとしたため、キューの内容をチェックする要求が中止された回数。
local time of last validate	最後の検証の実行が完了したときのローカル システム時刻。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内要素の検証を強制実行します。

show memory logging

ロギング用のメモリ使用状況を表示するには、特権 EXEC モードで **show memory logging** コマンドを使用します。

show memory logging [brief | wrap | include [address] [caller] [operator] [size] [process] [time] [context]]

構文の説明

address	（オプション）アドレス情報を表示します。
brief	（オプション）要約されたメモリ使用状況のロギングを表示します。
caller	（オプション）発信者情報を表示します。
コンテキスト	（オプション）仮想コンテキスト情報を表示します。
include	指定したフィールドのみを出力に含めます。任意の順序でフィールドを指定できますが、必ず次の順序で表示されます。 1. プロセス 2. 時刻 3. コンテキスト（シングル モード以外） 4. 処理（free/malloc/など） 5. アドレス 6. サイズ 7. 発信者 出力形式は、次のとおりです。 process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX 最大 4 つの発信者アドレスが表示されます。例に示すように、処理の種類（番号）が出力に列挙されます。
operator	（オプション）オペレータ情報を表示します。
process	（オプション）プロセス情報を表示します。
size	（オプション）サイズ情報を表示します。
time	（オプション）時間情報を表示します。
wrap	（オプション）メモリ使用状況のロギングのラップされたデータを表示します。これらの重複するデータが表示されたり保存されたりしないように、重複するデータは、このコマンドの入力後に消去されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが導入されました。

使用上のガイドライン

show memory logging コマンドは、ログのメモリ割り当てとメモリ使用状況を表示し、ユーザがメモリ ロギング ラップ イベントに対処できるようにします。

例

次に、ASA での **show memory logging** コマンドの出力例を示します。

```
ciscoasa# show memory logging

Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a

0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d

0x000000000182cc8a process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a

0x0000000000bff606 process=[CMGR Server Process] time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098 0x000000000182c08d
```

```
0x000000000182c262 process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b 0x000000000182c08d

0x000000000182c262 process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d

0x000000000182cc8a process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a

0x0000000000bff606 process=[CMGR Server Process] time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a

0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b
```

次に、ASA での **show memory logging include process operation size** コマンドの出力例を示します。

```
ciscoasa# show memory logging include process operation size
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free] size=72
process=
[CMGR Server Process] oper=[malloc] size=16 process=[CMGR Server Process] oper=[malloc]
size=512 process=[CMGR Server Process] oper=[free] size=512 process=[CMGR Server Process]
oper=[malloc] size=40 process=[CMGR Server Process] oper=[free] size=16 process=[CMGR
Server
Process] oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR
Server Process] oper=[malloc] size=512 process=[CMGR Server Process] oper=[free] size=512
process=[CMGR Server Process] oper=[malloc] size=40 process=[ci/console] oper=[malloc]
size=72
process=[ci/console] oper=[free] size=72
```

次に、ASA での **show memory logging brief** コマンドの出力例を示します。

```
ciscoasa# show memory logging brief
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
```

```
Number of malloc-fail                    0
Number of realloc-fail                   0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

関連コマンド

コマンド	説明
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory profile

ASA のメモリ使用率(プロファイリング)に関する情報を表示するには、特権 EXEC モードで **show memory profile** コマンドを使用します。

show memory profile [**peak**] [**detail** | **collated** | **status**]

構文の説明

collated	(任意)表示されるメモリ情報を整形します。
detail	(任意)メモリの詳細情報を表示します。
peak	(オプション)「使用中」のバッファではなく、ピーク キャプチャ バッファを表示します。
status	(任意)メモリ プロファイリングとピーク キャプチャ バッファの現在の状態を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show memory profile コマンドを使用して、メモリ使用状況レベルとメモリ リークをトラブルシューティングします。プロファイリングが停止されている場合でも、プロファイル バッファの内容を表示できます。プロファイリングを開始すると、バッファは自動的にクリアされます。

(注) メモリ プロファイリングをイネーブルにすると、ASA のパフォーマンスが一時的に低下する場合があります。

例

次に、**show memory profile** コマンドの出力例を示します。

```
ciscoasa# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

show memory profile detail コマンドの出力は、6 つのデータ列と 1 つのヘッダー列に区分され、左揃えで表示されています。ヘッダー列には、先頭のデータ列に対応するメモリ バケットのアドレスが表示されます(16 進数)。データ自体は、バケット アドレスにあるテキストまたはコードが保持しているバイト数です。データ カラム内のピリオド(.)は、このバケットのテキストによってメモリが保持されていないことを意味します。行内の他のカラムは、前のカラムから増分値に従って増分したバケット アドレスを表しています。たとえば、最初の行の先頭のデータ カラムのアドレス バケットは 0x001069e0 です。最初の行の 2 番めのデータ カラムのアドレス バケットは 0x001069e4 で、以降も同様に増分していきます。通常は、ヘッダー カラムにあるアドレスが次のバケット アドレスです。これは、前の行の最後のデータ カラムのアドレスに増分値を加算したものです。使用状況が含まれない行は表示されません。このような非表示になる行が、複数連続していることもあります。この場合は、ヘッダー カラムに 3 個のピリオド(...)で示されます。

次に、**show memory profile detail** コマンドの出力例を示します。

```
ciscoasa# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
<snip>
```

次に、**show memory profile collated** コマンドの出力例を示します。

```
ciscoasa# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

次に、**show memory profile peak** コマンドの出力例を示します。このコマンドでは、ピーク キャプチャ バッファを表示します。

```
ciscoasa# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

次に、**show memory profile peak detail** コマンドの出力例を示します。このコマンドでは、ピーク キャプチャ バッファと、対応するバケット アドレスにあるテキスト/コードが保持しているバイト数を表示します。

```
ciscoasa# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

次に、**show memory profile status** コマンドの出力例を示します。このコマンドでは、メモリ プロファイリングとピーク キャプチャ バッファの現在の状態を表示します。

```
ciscoasa# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況(メモリ プロファイリング)のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのプログラム テキスト範囲を設定します。
clear memory profile	メモリ プロファイリング機能によって保持されるメモリ バッファをクリアします。

show memory region

プロセス マップを表示するには、特権 EXEC モードで **show memory region** コマンドを使用します。

show memory region

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show memory region コマンドを使用すると、プロセス メモリ マップを表示できます。

例

次に、**show memory region** コマンドの出力例を示します。

```
ciscoasa# show memory region
ASLR enabled, text region 7f7397701000-7f739bc186c4

Address                   Perm Offset   Dev   Inode                     Pathname
7f7391a06000-7f7391d09000 rw-p 00000000 00:00 0                         [stack:2161]
7f7391d2a000-7f739212e000 rw-p 00000000 00:00 0                         [stack:2157]
7f7392530000-7f7392631000 rw-p 00000000 00:00 0                         [stack:2156]
7f7392647000-7f7392849000 rw-p 00000000 00:00 0                         [stack:2154]
7f7392895000-7f7392897000 r-xp 00000000 00:01 989                       /lib64/libutil-2.18.so
7f7392897000-7f7392a96000 ---p 00002000 00:01 989                       /lib64/libutil-2.18.so
7f7392a96000-7f7392a97000 r--p 00001000 00:01 989                       /lib64/libutil-2.18.so
7f7392a97000-7f7392a98000 rw-p 00002000 00:01 989                       /lib64/libutil-2.18.so
7f7392a98000-7f7392c9a000 r-xp 00000000 00:01 2923                      /usr/lib64/libcrypto.so.1.0.0
7f7392c9a000-7f7392e99000 ---p 00202000 00:01 2923                      /usr/lib64/libcrypto.so.1.0.0
7f7392e99000-7f7392ec3000 rw-p 00201000 00:01 2923                      /usr/lib64/libcrypto.so.1.0.0
7f7392ec7000-7f7392f28000 r-xp 00000000 00:01 3114                      /usr/lib64/libssl.so.1.0.0
7f7392f28000-7f7393127000 ---p 00061000 00:01 3114                      /usr/lib64/libssl.so.1.0.0
```

```
7f7393127000-7f7393132000 rw-p 00060000 00:01 3114                       /usr/lib64/libssl.so.1.0.0
7f7393132000-7f739316a000 r-xp 00000000 00:01 3202                       /usr/lib64/libxslt.so.1.1.28
7f739316a000-7f739336a000 ---p 00038000 00:01 3202                       /usr/lib64/libxslt.so.1.1.28
7f739336a000-7f739336c000 rw-p 00038000 00:01 3202                       /usr/lib64/libxslt.so.1.1.28
7f739336c000-7f73933ca000 r-xp 00000000 00:01 3439                       /usr/lib64/libxmlsec1.so.1.2.20
7f73933ca000-7f73935ca000 ---p 0005e000 00:01 3439                       /usr/lib64/libxmlsec1.so.1.2.20
7f73935ca000-7f73935ce000 rw-p 0005e000 00:01 3439                       /usr/lib64/libxmlsec1.so.1.2.20
7f73935ce000-7f7393606000 r-xp 00000000 00:01 2950
/usr/lib64/libxmlsec1-openssl.so.1.2.20
7f7393606000-7f7393805000 ---p 00038000 00:01 2950
/usr/lib64/libxmlsec1-openssl.so.1.2.20
7f7393805000-7f7393809000 rw-p 00037000 00:01 2950
/usr/lib64/libxmlsec1-openssl.so.1.2.20
7f739380a000-7f7393811000 r-xp 00000000 00:01 2976                       /usr/lib64/libffi.so.6.0.1
7f7393811000-7f7393a11000 ---p 00007000 00:01 2976                       /usr/lib64/libffi.so.6.0.1
7f7393a11000-7f7393a12000 rw-p 00007000 00:01 2976                       /usr/lib64/libffi.so.6.0.1
7f7393a12000-7f7393b94000 r-xp 00000000 00:01 2929                       /usr/lib64/libpython2.7.so.1.0
7f7393b94000-7f7393d94000 ---p 00182000 00:01 2929                       /usr/lib64/libpython2.7.so.1.0
7f7393d94000-7f7393dd3000 rw-p 00182000 00:01 2929                       /usr/lib64/libpython2.7.so.1.0
7f7393de1000-7f7393df6000 r-xp 00000000 00:01 948                        /lib64/libz.so.1.2.8
7f7393df6000-7f7393ff5000 ---p 00015000 00:01 948                        /lib64/libz.so.1.2.8
7f7393ff5000-7f7393ff6000 rw-p 00014000 00:01 948                        /lib64/libz.so.1.2.8
7f7393ff6000-7f739419a000 r-xp 00000000 00:01 961                        /lib64/libc-2.18.so
7f739419a000-7f7394399000 ---p 001a4000 00:01 961                        /lib64/libc-2.18.so
7f7394399000-7f739439d000 r--p 001a3000 00:01 961                        /lib64/libc-2.18.so
7f739439d000-7f739439f000 rw-p 001a7000 00:01 961                        /lib64/libc-2.18.so
7f73943a3000-7f73943b8000 r-xp 00000000 00:01 949                        /lib64/libgcc_s.so.1
7f73943b8000-7f73945b8000 ---p 00015000 00:01 949                        /lib64/libgcc_s.so.1
7f73945b8000-7f73945b9000 rw-p 00015000 00:01 949                        /lib64/libgcc_s.so.1
7f73945b9000-7f73946bb000 r-xp 00000000 00:01 999                        /lib64/libm-2.18.so
7f73946bb000-7f73948ba000 ---p 00102000 00:01 999                        /lib64/libm-2.18.so
7f73948ba000-7f73948bb000 r--p 00101000 00:01 999                        /lib64/libm-2.18.so
7f73948bb000-7f73948bc000 rw-p 00102000 00:01 999                        /lib64/libm-2.18.so
7f73948bc000-7f73948be000 r-xp 00000000 00:01 3641                       /asa/lib/libplatcap.so
7f73948be000-7f7394abd000 ---p 00002000 00:01 3641                       /asa/lib/libplatcap.so
7f7394abd000-7f7394ac5000 rw-p 00001000 00:01 3641                       /asa/lib/libplatcap.so
7f7394ac5000-7f7394b12000 r-xp 00000000 00:01 3213
/usr/lib64/libgobject-2.0.so.0.3600.4
7f7394b12000-7f7394d12000 ---p 0004d000 00:01 3213
/usr/lib64/libgobject-2.0.so.0.3600.4
7f7394d12000-7f7394d14000 rw-p 0004d000 00:01 3213
/usr/lib64/libgobject-2.0.so.0.3600.4
7f7394d14000-7f7394e3d000 r-xp 00000000 00:01 3120                       /usr/lib64/libglib-2.0.so.0.3600.4
7f7394e3d000-7f739503d000 ---p 00129000 00:01 3120                       /usr/lib64/libglib-2.0.so.0.3600.4
7f739503d000-7f739503f000 rw-p 00129000 00:01 3120                       /usr/lib64/libglib-2.0.so.0.3600.4
7f739503f000-7f73950ce000 r-xp 00000000 00:01 3143                       /usr/lib64/liblasso.so.3.11.1
7f73950ce000-7f73952ce000 ---p 0008f000 00:01 3143                       /usr/lib64/liblasso.so.3.11.1
7f73952ce000-7f73952d9000 rw-p 0008f000 00:01 3143                       /usr/lib64/liblasso.so.3.11.1
7f73952d9000-7f73952e9000 r-xp 00000000 00:01 3175                       /usr/lib64/libprotobuf-c.so.0.0.0
7f73952e9000-7f73954e8000 ---p 00010000 00:01 3175                       /usr/lib64/libprotobuf-c.so.0.0.0
7f73954e8000-7f73954e9000 rw-p 0000f000 00:01 3175                       /usr/lib64/libprotobuf-c.so.0.0.0
7f73954e9000-7f739551b000 r-xp 00000000 00:01 3629                       /asa/lib/libmsglyr.so
7f739551b000-7f739571b000 ---p 00032000 00:01 3629                       /asa/lib/libmsglyr.so
7f739571b000-7f7395720000 rw-p 00032000 00:01 3629                       /asa/lib/libmsglyr.so
7f7395720000-7f739576c000 r-xp 00000000 00:01 3146                       /usr/lib64/libzmq.so.3.1.0
7f739576c000-7f739596c000 ---p 0004c000 00:01 3146                       /usr/lib64/libzmq.so.3.1.0
7f739596c000-7f7395970000 rw-p 0004c000 00:01 3146                       /usr/lib64/libzmq.so.3.1.0
7f7395970000-7f7395ac0000 r-xp 00000000 00:01 2952                       /usr/lib64/libxml2.so.2.9.1
7f7395ac0000-7f7395cc0000 ---p 00150000 00:01 2952                       /usr/lib64/libxml2.so.2.9.1
7f7395cc0000-7f7395cca000 rw-p 00150000 00:01 2952                       /usr/lib64/libxml2.so.2.9.1
7f7395ccb000-7f7395ceb000 r-xp 00000000 00:01 3628                       /asa/lib/libpdts.so
7f7395ceb000-7f7395eea000 ---p 00020000 00:01 3628                       /asa/lib/libpdts.so
7f7395eea000-7f7395eec000 rw-p 0001f000 00:01 3628                       /asa/lib/libpdts.so
7f7395eec000-7f7395eff000 r-xp 00000000 00:01 2057                       /lib64/libresolv-2.18.so
```

```
7f7395eff000-7f73960ff000 ---p 00013000 00:01 2057                       /lib64/libresolv-2.18.so
7f73960ff000-7f7396100000 r--p 00013000 00:01 2057                       /lib64/libresolv-2.18.so
7f7396100000-7f7396101000 rw-p 00014000 00:01 2057                       /lib64/libresolv-2.18.so
7f7396103000-7f7396110000 r-xp 00000000 00:01 955                        /lib64/libudev.so.0.13.1
7f7396110000-7f739630f000 ---p 0000d000 00:01 955                        /lib64/libudev.so.0.13.1
7f739630f000-7f7396310000 rw-p 0000c000 00:01 955                        /lib64/libudev.so.0.13.1
7f7396310000-7f7396322000 r-xp 00000000 00:01 964                        /lib64/libcgroup.so.1.0.38
7f7396322000-7f7396521000 ---p 00012000 00:01 964                        /lib64/libcgroup.so.1.0.38
7f7396521000-7f7396523000 rw-p 00011000 00:01 964                        /lib64/libcgroup.so.1.0.38
7f739677d000-7f7396784000 r-xp 00000000 00:01 2067                       /lib64/librt-2.18.so
7f7396784000-7f7396983000 ---p 00007000 00:01 2067                       /lib64/librt-2.18.so
7f7396983000-7f7396984000 r--p 00006000 00:01 2067                       /lib64/librt-2.18.so
7f7396984000-7f7396985000 rw-p 00007000 00:01 2067                       /lib64/librt-2.18.so
7f7396985000-7f7396988000 r-xp 00000000 00:01 2060                       /lib64/libdl-2.18.so
7f7396988000-7f7396b87000 ---p 00003000 00:01 2060                       /lib64/libdl-2.18.so
7f7396b87000-7f7396b88000 r--p 00002000 00:01 2060                       /lib64/libdl-2.18.so
7f7396b88000-7f7396b89000 rw-p 00003000 00:01 2060                       /lib64/libdl-2.18.so
7f7396b89000-7f7396ba2000 r-xp 00000000 00:01 1001                       /lib64/libpthread-2.18.so
7f7396ba2000-7f7396da1000 ---p 00019000 00:01 1001                       /lib64/libpthread-2.18.so
7f7396da1000-7f7396da2000 r--p 00018000 00:01 1001                       /lib64/libpthread-2.18.so
7f7396da2000-7f7396da3000 rw-p 00019000 00:01 1001                       /lib64/libpthread-2.18.so
7f7396da7000-7f7396dce000 r-xp 00000000 00:01 3434                       /usr/lib64/libexpat.so.1.6.0
7f7396dce000-7f7396fcd000 ---p 00027000 00:01 3434                       /usr/lib64/libexpat.so.1.6.0
7f7396fcd000-7f7396fd0000 rw-p 00026000 00:01 3434                       /usr/lib64/libexpat.so.1.6.0
7f7396fd0000-7f73970b6000 r-xp 00000000 00:01 3113                       /usr/lib64/libstdc++.so.6.0.18
7f73970b6000-7f73972b5000 ---p 000e6000 00:01 3113                       /usr/lib64/libstdc++.so.6.0.18
7f73972b5000-7f73972bd000 r--p 000e5000 00:01 3113                       /usr/lib64/libstdc++.so.6.0.18
7f73972bd000-7f73972bf000 rw-p 000ed000 00:01 3113                       /usr/lib64/libstdc++.so.6.0.18
7f73972d4000-7f73972de000 r-xp 00000000 00:01 3174                       /usr/lib64/libnuma.so.1
7f73972de000-7f73974dd000 ---p 0000a000 00:01 3174                       /usr/lib64/libnuma.so.1
7f73974dd000-7f73974de000 rw-p 00009000 00:01 3174                       /usr/lib64/libnuma.so.1
7f73974de000-7f73974fe000 r-xp 00000000 00:01 950                        /lib64/ld-2.18.so
7f73976fe000-7f73976ff000 r--p 00020000 00:01 950                        /lib64/ld-2.18.so
7f73976ff000-7f7397700000 rw-p 00021000 00:01 950                        /lib64/ld-2.18.so
7f7397701000-7f739bc19000 r-xp 00000000 00:01 3650                       /asa/bin/lina
7f739be18000-7f739cc16000 rw-p 04517000 00:01 3650                       /asa/bin/lina
7ffffe1fc000-7ffffe21d000 rw-p 00000000 00:00 0                          [stack]
7ffffe2f1000-7ffffe2f3000 r-xp 00000000 00:00 0                          [vdso]
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況(メモリ プロファイリング)のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのプログラム テキスト範囲を設定します。
clear memory profile	メモリ プロファイリング機能によって保持されるメモリ バッファをクリアします。

show memory top-usage

show memory detail コマンドから割り当てられたフラグメント サイズの上位いくつかを表示するには、特権 EXEC モードで **show memory top-usage** コマンドを使用します。

show memory top-usage [*num*]

構文の説明

num	（オプション）リストにバイナリ サイズの数を表示します。有効な値は 1 ～ 64 です。

デフォルト

num のデフォルトは 10 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(6)	このコマンドが追加されました。

使用上のガイドライン

show memory detail コマンドから割り当てられたフラグメント サイズの上位いくつかを表示するには、**show memory top-usage** コマンドを使用します。

このコマンドは、クラスタリングを使用しません。クラスタリングがイネーブルの場合にクラスタリングをディセーブルにする必要はありません。

例

次に、**show memory top-usage** コマンドの出力例を示します。

```
ciscoasa# show memory top-usage 3
MEMPOOL_DMA pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
      1572864             9       14155776
     12582912             1       12582912
      6291456             1        6291456
```

```
----- Binsize PC top usage -----

Binsize: 1572864                total (bytes): 14155776

pc = 0x805a870, size = 16422399 , count = 9

Binsize: 12582912               total (bytes): 12582912

pc = 0x805a870, size = 12960071 , count = 1

Binsize: 6291456                total (bytes): 6291456

pc = 0x9828a6c, size = 7962695  , count = 1


MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
     12582912             1       12582912
      2097152             6       12582912
        65536           181       11862016

----- Binsize PC top usage -----

Binsize: 12582912               total (bytes): 12582912

pc = 0x8249763, size = 37748736 , count = 1

Binsize: 2097152                total (bytes): 12582912

pc = 0x8a7ebfb, size = 2560064  , count = 1
pc = 0x8aa4413, size = 2240064  , count = 1
pc = 0x8a9bb13, size = 2240064  , count = 1
pc = 0x8a80542, size = 2097152  , count = 1
pc = 0x97e7172, size = 2097287  , count = 1
pc = 0x8996463, size = 2272832  , count = 1

Binsize: 65536                  total (bytes): 11862016

pc = 0x913db2b, size = 11635232 , count = 161
pc = 0x91421eb, size = 138688   , count = 2
pc = 0x97e7172, size = 339740   , count = 4
pc = 0x97e7433, size = 197229   , count = 3
pc = 0x82c3412, size = 65536    , count = 1
pc = 0x8190e09, size = 155648   , count = 2
pc = 0x8190af6, size = 77824    , count = 1
pc = 0x93016a1, size = 65536    , count = 1
pc = 0x89f1a40, size = 65536    , count = 1
pc = 0x9131140, size = 163968   , count = 2
pc = 0x8ee56c8, size = 66048    , count = 1
pc = 0x8056a01, size = 66528    , count = 1
pc = 0x80569e5, size = 66528    , count = 1
```

関連コマンド

コマンド	説明
show memory tracking	現在収集されているすべての情報を表示します。

show memory tracking

ツールによって追跡される、現在割り当て済みのメモリを表示するには、特権 EXEC モードで **show memory tracking** コマンドを実行します。

show memory tracking [**address** | **dump** | **detail**]

構文の説明

address	(任意)アドレスごとのメモリのトラッキングを表示します。
detail	(オプション)内部メモリのトラッキング状態を表示します。
dump	(オプション)メモリのトラッキング アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

show memory tracking コマンドを使用して、ツールにより追跡されている、現在割り当て済みのメモリを表示します。

例

次に、**show memory tracking** コマンドの出力例を示します。

```
ciscoasa# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

次に、**show memory tracking address** コマンドの出力例を示します。

```
ciscoasa# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

```
memory tracking by address:
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
57 byte region @ 0xa893aed0 allocated by 0x080c5125
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2
```

次に、**show memory tracking dump** コマンドの出力例を示します。

```
ciscoasa# show memory tracking dump
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aee0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aef0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893af00: 0c 0c 0c 0c 0c 0c 0c 0c 0c | .........
```

関連コマンド

コマンド	説明
clear memory tracking	現在収集されているすべての情報をクリアします。

show memory utilization

Show memory utilization コマンドを使用して、ASA に設定されているリロードしきい値の制限とクラッシュ情報を表示します。

show memory-utilization [reload-threshold]

構文の説明

reload-threshold	設定されているシステム メモリのリロードしきい値の制限、および、システムのリロードの前にクラッシュ情報が保存されているかどうかを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

リロードしきい値が設定されているかどうかを確認するには、**show memory utilization**コマンドを使用します。設定されている場合は、しきい値の制限と、リロードが設定される前にクラッシュ情報を保存するオプションを選択するかどうかを確認できます。

例

次に、ASA 上にメモリ使用状況機能を設定する例を示します。

```
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is not configured.

ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is configured:
Reload at: 93%
Crashinfo Generation: yes

ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is configured:
Reload at: 90%
Crashinfo Generation: no
```

show memory webvpn

WebVPN のメモリ使用状況の統計情報を生成するには、特権 EXEC モードで **show memory webvpn** コマンドを使用します。

show memory webvpn [**allobjects** | **blocks** | **dumpstate** [**cache** | **disk0** | **disk1** | **flash** | **ftp** | **system** | **tftp**] | **pools** | **profile** [**clear** | **dump** | **start** | **stop**] | **usedobjects** {{**begin** | **exclude** | **grep** | **include**} **line** *line*}]

構文の説明

allobjects	プール、ブロック、すべての使用済みオブジェクトおよび解放済みオブジェクトについて、WebVPN メモリ使用量の詳細を表示します。
begin	一致する行から開始します。
blocks	メモリ ブロックについて、WebVPN メモリ使用量の詳細を表示します。
cache	WebVPN メモリ キャッシュ状態のダンプのファイル名を指定します。
clear	WebVPN メモリ プロファイルをクリアします。
disk0	WebVPN メモリ disk0 状態のダンプのファイル名を指定します。
disk1	WebVPN メモリ disk1 状態のダンプのファイル名を指定します。
dump	WebVPN メモリ プロファイルをファイルに出力します。
dumpstate	WebVPN メモリ状態をファイルに出力します。
exclude	一致する行を除外します。
flash	WebVPN メモリ フラッシュ状態のダンプのファイル名を指定します。
ftp	WebVPN メモリ FTP 状態のダンプのファイル名を指定します。
grep	一致する行を含めるか、または除外します。
include	一致する行を含めます。
line	一致する行を特定します。
line	一致する行を指定します。
プール	メモリ プールについて、WebVPN メモリ使用量の詳細を表示します。
プロファイル	WebVPN メモリ プロファイルを収集して、ファイルに出力します。
system	WebVPN メモリ システム状態のダンプのファイル名を指定します。
start	WebVPN メモリ プロファイルの収集を開始します。
stop	WebVPN メモリ プロファイルの収集を停止します。
tftp	WebVPN メモリ TFTP 状態のダンプのファイル名を指定します。
usedobjects	使用済みオブジェクトについて、WebVPN メモリ使用量の詳細を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

例

次に、**show memory webvpn allobjects** コマンドの出力例を示します。

```
ciscoasa# show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

関連コマンド

コマンド	説明
memory-size	WebVPN が使用できる ASA のメモリ量を設定します。

show mfib

転送エントリおよびインターフェイスの観点から MFIB を表示するには、特権 EXEC モードで **show mfib** コマンドを使用します。

show mfib [*group* [*source*]] [**verbose**] [**cluster**]

構文の説明

クラスタ	(オプション)MFIB のエポック番号と現在のタイマー値を表示します。
group	(オプション)マルチキャスト グループの IP アドレスを表示します。
source	(オプション)マルチキャスト ルートの送信元の IP アドレスを表示します。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。
verbose	(任意)エントリに関する追加情報を表示します。

デフォルト

任意の引数を指定しないと、すべてのグループの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	**cluster** キーワードが追加されました。ASA 5580 および 5585-X にのみ適用されます。

例

次に、**show mfib** コマンドの出力例を示します。

```
ciscoasa# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib verbose	転送エントリおよびインターフェイスに関する詳細情報を表示します。

show mfib active

アクティブなマルチキャスト送信元を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib active** コマンドを使用します。

show mfib [*group*] **active** [*kbps*]

構文の説明

group	(任意)マルチキャスト グループの IP アドレスです。
kbps	(任意)この値以上のマルチキャスト ストリームのみに表示を制限します。

このコマンドには引数またはキーワードはありません。

デフォルト

kbps のデフォルト値は 4 です。*group* を指定しない場合、すべてのグループが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show mfib active コマンドの出力では、PPS のレートに正または負の数値が表示されます。ASA が負の数値を表示するのは、RPF パケットが失敗した場合か、ルータが発信インターフェイス(OIF)リストを使用して RPF パケットをモニタしている場合です。このような現象が発生している場合は、マルチキャスト ルーティングに問題がある可能性があります。

例

次に、**show mfib active** コマンドの出力例を示します。

```
ciscoasa# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)
```

```
Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

関連コマンド

コマンド	説明
show mroute active	アクティブなマルチキャスト ストリームを表示します。

show mfib count

MFIB ルートとパケット数データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib count** コマンドを使用します。

show mfib [*group* [*source*]] **count**

構文の説明

group	（任意）マルチキャスト グループの IP アドレスです。
source	（任意）マルチキャスト ルート送信元の IP アドレスです。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、パケットのドロップに関する統計情報を表示します。

例

次に、**show mfib count** コマンドの出力例を示します。

```
ciscoasa# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

関連コマンド

コマンド	説明
clear mfib counters	MFIB ルータ パケット カウンタをクリアします。
show mroute count	マルチキャスト ルート カウンタを表示します。

show mfib interface

MFIB プロセスに関係しているインターフェイスのパケット統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib interface** コマンドを使用します。

show mfib interface [*interface*]

構文の説明

interface	(任意)インターフェイス名。指定されたインターフェイスのみに表示を制限します。

デフォルト

すべての MFIB インターフェイスの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show mfib interface** コマンドの出力例を示します。

```
ciscoasa# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib reserved

予約済みグループを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib reserved** コマンドを使用します。

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

構文の説明

active	（任意）アクティブなマルチキャスト送信元を表示します。
count	（任意）パケットおよびルートの数に関するデータを表示します。
kpbs	（オプション）この値以上のアクティブなマルチキャスト送信元に表示を制限します。
verbose	（任意）追加情報を表示します。

デフォルト

kbps のデフォルト値は 4 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、224.0.0.0 ～ 224.0.0.225 の範囲の MFIB エントリを表示します。

例

次に、**show mfib reserved** コマンドの出力例を示します。

```
ciscoasa# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface
Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
```

```
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
   inside Flags: IC
```

関連コマンド

コマンド	説明
show mfib active	アクティブなマルチキャスト ストリームを表示します。

show mfib status

MFIB の全般的なコンフィギュレーションと動作ステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib status** コマンドを使用します。

show mfib status

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show mfib status** コマンドの出力例を示します。

```
ciscoasa# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib summary

MFIB のエントリとインターフェイスの数に関する要約情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib summary** コマンドを使用します。

show mfib summary

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show mfib summary** コマンドの出力例を示します。

```
ciscoasa# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

関連コマンド

コマンド	説明
show mroute summary	マルチキャスト ルーティング テーブルの要約情報を表示します。

show mfib verbose

転送エントリとインターフェイスに関する詳細情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib verbose** コマンドを使用します。

show mfib verbose

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show mfib verbose** コマンドの出力例を示します。

```
ciscoasa# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。
show mfib summary	MFIB のエントリとインターフェイスの数に関する要約情報を表示します。

show mgcp

MGCP のコンフィギュレーションとセッション情報を表示するには、特権 EXEC モードで **show mgcp** コマンドを使用します。

show mgcp {**commands** | **sessions**} [**detail**]

構文の説明

コマンド	コマンド キュー内の MGCP コマンドの数を表示します。
detail	(任意)各コマンド(またはセッション)に関する追加情報を出力に表示します。
sessions	既存の MGCP セッションの数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show mgcp commands コマンドは、コマンド キュー内の MGCP コマンド数を表示します。**show mgcp sessions** コマンドは、既存の MGCP セッション数を表示します。**detail** オプションは、各コマンド(またはセッション)に関する追加情報を出力に含めます。

例

次に、**show mgcp** コマンド オプションの例を示します。

```
ciscoasa# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
ciscoasa#

ciscoasa# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP | host-pc-2
        Transaction ID  2052
        Endpoint name | aaln/1
        Call ID | 9876543210abcdef
```

```
        Connection ID|
        Media IP|192.168.5.7
        Media port|6058
ciscoasa#

ciscoasa# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
ciscoasa#

ciscoasa# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP|host-pc-2
        Call ID|9876543210abcdef
        Connection ID|6789af54c9
        Endpoint name|aaln/1
        Media lcl port  6166
        Media rmt IP|192.168.5.7
        Media rmt port  6058
ciscoasa#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug mgcp	MGCP のデバッグ情報をイネーブルにします。
inspect mgcp	MGCP アプリケーション インスペクションをイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。

show mmp

既存の MMP セッションに関する情報を表示するには、特権 EXEC モードで **show mmp** コマンドを使用します。

show mmp [*address*]

構文の説明

address	MMP クライアント/サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、既存の MMP セッションに関する情報を表示する **show mmp** コマンドの使用例を示します。

```
ciscoasa# show mmp 10.0.0.42
MMP session:: inside:10.0.0.42/5443 outside:172.23.62.204/2442
session-id=71AD3EB1-7BE8-42E0-8DC3-E96E41D4ADD5
data:: rx-bytes=1258, tx-bytes=1258
```

関連コマンド

コマンド	説明
debug mmp	MMP 検査イベントを表示します。
inspect mmp	MMP インスペクション エンジンを設定します。
show debug mmp	MMP インスペクション モジュールの現在のデバッグ設定を表示します。

show mode

実行中のソフトウェア イメージ、およびフラッシュ メモリ内の任意のイメージのためのセキュリティ コンテキスト モードを表示するには、特権 EXEC モードで **show mode** コマンドを使用します。

show mode

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show mode** コマンドの出力例を示します。次に、現在のモードと、実行されていないイメージ「image.bin」のモードの例を示します。

```
ciscoasa# show mode flash:/image.bin
Firewall mode: multiple
```

モードは、マルチまたはシングルのいずれかです。

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
mode	コンテキスト モードをシングルまたはマルチに設定します。

show module

ASA にインストールされているモジュールに関する情報を表示するには、ユーザ EXEC モードで **show module** コマンドを使用します。

show module [*id* | **all**] [**details** | **recover** | **log** [**console**]

構文の説明

all	(デフォルト)すべてのモジュールの情報を表示します。
console	(オプション)モジュールのコンソール ログ情報を表示します。
details	(オプション)モジュールのリモート管理設定などの追加情報を表示します。
id	モジュール ID を指定します。ハードウェア モジュールの場合、**0**(ASA の場合)または **1**(インストールされたモジュールの場合)のいずれかのスロット番号を指定します。ソフトウェア モジュールの場合、次の名前のいずれかを指定します。 • **sfr**:ASA FirePOWER モジュール。 • **ips**:IPS モジュール • **cxsc**:ASA CX モジュール
ログ	(オプション)モジュールのログ情報を表示します。
recover	(オプション)**hw-module** または **sw-module module recover** コマンドの設定を表示します。

デフォルト

デフォルトでは、すべてのモジュールの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト[1]	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

1. **show module recover** コマンドは、システム実行スペースでのみ使用できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、より多くの詳細情報を出力するように変更されました。
8.2(1)	SSC に関する情報が出力に含まれています。
8.2(5)	ASA 5585-X と、ASA 5585-X 上の IPS SSP のサポートに関する情報が追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。

リリース	変更内容
8.6(1)	ASA 5512-X ～ ASA 5555-X では、**log** および **console** キーワードが追加されました。さらに、**ips** のデバイス ID が追加されました。
9.1(1)	ASA CX ソフトウェア モジュールのサポートが、**cxsc** モジュール ID の追加によって追加されました。
9.2(1)	**sfr** キーワードを含め、ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、ASA にインストールされているモジュールに関する情報を表示します。ASA 自体もディスプレイにモジュールとして表示されます(スロット 0)。

例

次に、**show module** コマンドの出力例を示します。モジュール 0 はベース デバイス。モジュール 1 は CSC SSM です。

```
ciscoasa# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0 (Build#1187)

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

次の表に、出力に表示される各フィールドを示します。

表 9-12　show module の出力フィールド

フィールド	説明
Mod	モジュール番号、0 または 1。
ポート	ポート番号。
Card Type	モジュール 0 に表示されるデバイスの場合、タイプはプラットフォーム モデルです。モジュール 1 の SSM の場合、タイプは SSM タイプです。
モデル	このモジュールのモデル番号。
Serial No.	シリアル番号。
MAC Address Range	この SSM、またはデバイス、組み込みインターフェイスの MAC アドレス範囲。
Hw Version	ハードウェアのバージョン。
Fw Version	ファームウェアのバージョン。

表 9-12　show module の出力フィールド(続き)

フィールド	説明
Sw Version	ソフトウェアのバージョン。
SSM Application Name	SSM で実行されているアプリケーションの名前。
SSM Application Version	SSM で実行されているアプリケーションのバージョン。
Status(ステータス)	モジュール 0 のデバイスの場合、ステータスは Up Sys です。モジュール 1 の SSM のステータスは、次のいずれかです。 • Initializing:SSM が検出され、デバイスによってコントロール通信が初期化されます。 • Up:SSM がデバイスによる初期化を完了しました。 • Unresponsive:この SSM との通信中にデバイスでエラーが発生しました。 • Reloading:SSM がリロード中です。 • Shutting Down:SSM をシャットダウンしています。 • Down:SSM がシャットダウンされました。 • Recover:SSM が回復イメージをダウンロードしようとしています。 • No Image Present:IPS ソフトウェアがインストールされていません。
Data Plane Status	データ プレーンの現在の状態。
互換性	残りのデバイスに関連した SSM の互換性。
スロット	物理スロット番号(デュアル SSP モードでのみ有効)。

show module details コマンドの出力は、インストールされているモジュールによって異なります。たとえば、CSC SSM の出力には CSC SSM ソフトウェアのコンポーネントに関するフィールドが含まれます。

次に、**show module 1 details** コマンドの出力例を示します。

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

次の表に、出力の追加フィールドを示します。

表 9-13　show module details の追加出力フィールド

フィールド	説明
DC address （表示なし）	（ASA FirePOWER のみ）。モジュールを管理する Firepower Management Center のアドレス。
Mgmt IP addr	モジュールの管理インターフェイスの IP アドレスを表示します。
Mgmt Network Mask （表示なし）	管理アドレスのサブネット マスクを表示します。
Mgmt Gateway （表示なし）	管理アドレスのゲートウェイ。
Mgmt web ports	モジュールの管理インターフェイスに設定されたポートを表示します。
Mgmt TLS enabled	モジュールの管理インターフェイスの接続に対して Transport Layer Security がイネーブルであるかどうか（True または False）を表示します。

ソフトウェア モジュールを設定できるモデルの場合、**show module** コマンドは可能なすべてのモジュールを表示します。ステータス情報は、これらの 1 つがインストールされているかどうかを表示します。

```
ciscoasa# show module

Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt     ASA5555            FCH1714J6HP
 ips Unknown                                      N/A                FCH1714J6HP
cxsc Unknown                                      N/A                FCH1714J6HP
 sfr FirePOWER Services Software Module           ASA5555            FCH1714J6HP

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 bc16.6520.1dcd to bc16.6520.1dd6  1.0          2.1(9)8      100.8(66)11
 ips bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
cxsc bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
 sfr bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A          5.3.1-100

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 ips Unknown                        No Image Present Not Applicable
cxsc Unknown                        No Image Present Not Applicable
 sfr ASA FirePOWER                  Up               5.3.1-100

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
 ips Unresponsive       Not Applicable
cxsc Unresponsive       Not Applicable
 sfr Up                 Up

Mod  License Name   License Status  Time Remaining
---- -------------- --------------- ---------------
 ips IPS Module     Enabled         172 days
```

次に、**show module 1 recover** コマンドの出力例を示します。

```
ciscoasa# show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

次に、SSC がインストールされているときの **show module 1 details** コマンドの出力例を示します。

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5505 Security Services Card
Model: ASA-SSC
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc:
App. Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

次に、ASA 5585-X に IPS SSP がインストールされているときの **show module 1 details** コマンドの出力例を示します。

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA-SSM-20
Hardware version: V1.0
Serial Number: 12345678
Firmware version: 1.0(7)2
Software version: 4.1(1.1)S47(0.1)
MAC Address Range: 000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status: Up
Status: Up
Mgmt IP addr: 10.89.147.13
Mgmt web ports: 443
Mgmt TLS enabled: true
```

次に、ASA 5585-X に CXSC SSP がインストールされているときの **show module all** コマンドの出力例を示します。

```
ciscoasa# show module all

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1504CBRM
  1 ASA 5585-X CXSC Security Services Processor-1 ASA5585-SSP-IPS10  JAF1510BLSE

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
```

```
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1d54 to 5475.d05b.1d5f  1.0          2.0(7)0      100.7(14)13
  1 5475.d05b.248c to 5475.d05b.2497  1.0          0.0(0)0      1.0

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CXSC Security Module             Up               1.0

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

次に、ASA 5585-X に CXSC SSP がインストールされているときの **show module 1 details** コマンドの出力例を示します。

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA5585-S10C10-K8
Hardware version:   1.0
Serial Number:      123456789
Firmware version:   1.0(9)0
Software version:   CXSC Security Module Version 1.0
App. name:          CXSC Security Module
App. version:       Version 1.0
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Activated:          Yes
Mgmt IP addr:       100.0.1.4
Mgmt web port:      8443
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	回復イメージを TFTP サーバからロードして、モジュールを回復します。
hw-module module reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るための準備として、モジュール ソフトウェアを閉じます。
sw-module	ソフトウェア モジュールを設定します。

show monitor-interface

フェールオーバーのためにモニタ対象にするインターフェイスの情報を表示するには、特権 EXEC モードで **show monitor-interface** コマンドを使用します。

show monitor-interface

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(2)	IPv6 アドレスが出力に追加されました。

使用上のガイドライン

インターフェイスには複数の IPv6 アドレスを設定できるため、**show monitor-interface** コマンドではリンクローカル アドレスのみが表示されます。IPv4 と IPv6 の両方のアドレスがインターフェイスで設定されている場合は、両方のアドレスが出力に表示されます。インターフェイスに IPv4 アドレスが設定されていない場合、出力の IPv4 アドレスは 0.0.0.0 として表示されます。インターフェイスに IPv6 アドレスが設定されていない場合、アドレスは単純に出力から省かれます。

モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Normal (Waiting)：インターフェイスは起動していますが、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。インターフェイスのスタンバイ IP アドレスが設定されていること、および 2 つのインターフェイス間の接続が存在することを確認してください。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。

- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

例

次に、**show monitor-interface** コマンドの出力例を示します。

```
ciscoasa# show monitor-interface

This host: Primary - Active
                Interface outside (10.86.94.88): Normal (Waiting)
                Interface management (192.168.1.1): Normal (Waiting)
                Interface failif (0.0.0.0/fe80::223:4ff:fe77:fed): Normal (Waiting)
        Other host: Secondary - Failed
                Interface outside (0.0.0.0): Unknown (Waiting)
                Interface management (0.0.0.0): Unknown (Waiting)
                Interface failif (0.0.0.0): Unknown (Waiting)
```

関連コマンド

コマンド	説明
monitor-interface	特定のインターフェイスでのヘルス モニタリングをイネーブルにします。

show mrib client

MRIB クライアント接続に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib client** コマンドを使用します。

show mrib client [**filter**] [**name** *client_name*]

構文の説明

filter	(任意)クライアント フィルタを表示します。各クライアントが所有する MRIB フラグと、各クライアントが関連するフラグに関する情報を表示するために使用します。
name *client_name*	(任意)PIM または IGMP など、MRIB のクライアントとして動作するマルチキャスト ルーティング プロトコルの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

filter オプションを使用して、さまざまな MRIB クライアントが登録されているルートおよびインターフェイス レベル フラグの変更を表示します。このコマンド オプションからは、MRIB クライアントが所有するフラグも表示されます。

例

次に、**filter** キーワードを使用した **show mrib client** コマンドの出力例を示します。

```
ciscoasa# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
```

```
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルのエントリを表示します。

show mrib route

MRIB テーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib route** コマンドを使用します。

show mrib route [[*source* | *****] [*group*[*/prefix-length*]]]

構文の説明

*	(任意)共有ツリー エントリを表示します。
/prefix-length	(任意)MRIB ルートのプレフィックス長。プレフィックス(アドレスのネットワーク部分)を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
group	(任意)グループの IP アドレスまたは名前。
source	(任意)ルート送信元の IP アドレスまたは名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

MFIB テーブルには、MRIB から更新されるエントリとフラグのサブセットが保持されます。フラグは、マルチキャスト パケットの転送ルールのセットに従って、転送およびシグナリングの動作を決定します。

インターフェイスとフラグのリストに加えて、各ルート エントリにはさまざまなカウンタが表示されます。バイト数は、転送されたバイトの合計数です。パケット数は、このエントリについて受信されたパケット数です。**show mfib count** コマンドは、ルートとは無関係にグローバルなカウンタを表示します。

例

次に、**show mrib route** コマンドの出力例を示します。

```
ciscoasa# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

関連コマンド

コマンド	説明
show mfib count	MFIB テーブルのルートとパケット数データを表示します。
show mrib route summary	MRIB テーブル エントリの要約を表示します。

show mroute

IPv4 マルチキャスト ルーティング テーブルを表示するには、特権 EXEC モードで **show mroute** コマンドを使用します。

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

構文の説明

active *rate*	(任意)アクティブなマルチキャスト送信元のみを表示します。アクティブな送信元とは、指定された *rate* 以上で送信を実行している送信元です。*rate* が指定されていない場合、アクティブな送信元は 4 kbps 以上のレートで送信を実行している送信元です。
count	(任意)グループと送信元に関する統計情報を表示します。この情報には、パケットの数、1 秒あたりのパケット数、パケットの平均サイズ、および 1 秒あたりのビット数が含まれています。
group	(任意)DNS ホスト テーブルで定義されているマルチキャスト グループの IP アドレスまたは名前。
pruned	(任意)プルーニングされたルートを表示します。
reserved	(任意)予約済みグループを表示します。
source	(任意)送信元のホスト名または IP アドレス。
summary	(任意)マルチキャスト ルーティング テーブル内の各エントリの要約を 1 行で表示します。

デフォルト

rate 引数を指定しない場合、デフォルトでは 4 Kbps になります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show mroute コマンドは、マルチキャスト ルーティングの内容を表示します。ASA は、PIM プロトコル メッセージ、IGMP レポート、およびトラフィックに基づいて (S,G) および (*,G) エントリを作成して、マルチキャスト ルーティング テーブルにデータを入力します。アスタリスク (*) は、すべての送信元アドレスを示し、「S」は単一ソース アドレスを示し、「G」は宛先マルチキャスト グループ アドレスを示します。(S,G) エントリを作成する場合、ソフトウェアはユニキャスト ルーティング テーブル内で (RPF を経由して) 見つかった宛先グループへの最適パスを使用します。

実行コンフィギュレーションに含まれている **mroute** コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**show mroute** コマンドの出力例を示します。

```
ciscoasa(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

show mroute の出力には、次のフィールドが含まれています。

- **Flags**: エントリに関する情報を提供します。
  - **D (Dense)**: エントリはデンス モードで動作しています。
  - **S (Sparse)**: エントリはスパース モードで動作しています。
  - **B (Bidir Group)**: マルチキャスト グループが双方向モードで動作していることを示します。
  - **s (SSM Group)**: マルチキャスト グループが SSM の IP アドレス範囲内であることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。
  - **C (Connected)**: マルチキャスト グループのメンバーは、直接接続されたインターフェイス上に存在します。
  - **L (Local)**: ASA 自体が、マルチキャスト グループのメンバーです。グループは、(設定済みのグループに対する) **igmp join-group** コマンドによってローカルに加入されています。
  - **I (Received Source Specific Host Report)**: (S,G) エントリが (S,G) レポートによって作成されたことを示します。この (S,G) レポートは IGMP によって作成された可能性があります。このフラグが設定されるのは、DR に対してのみです。

  - **P（Pruned）**：ルートがプルーニングされています。ソフトウェアは、この情報を保持して、ダウンストリーム メンバーが送信元に加入できるようにします。
  - **R（RP-bit set）**：(S,G) エントリが RP をポイントしていることを示します。
  - **F（Register flag）**：ソフトウェアがマルチキャスト送信元に登録されていることを示します。
  - **T（SPT-bit set）**：パケットが最短パス送信元ツリーで受信されていることを示します。
  - **J（Join SPT）**：(*, G) エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します（デフォルトの SPT しきい値設定は 0 kbps です）。J - Join 最短パス ツリー（SPT）フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方向に (S,G) join がトリガーされます。これにより、ASA は送信元ツリーに加入します。

    (S, G) エントリの場合、グループの SPT しきい値を超過したためにエントリが作成されたことを示します。(S,G) エントリに J - Join SPT フラグが設定されている場合、ASA は送信元ツリー上のトラフィック速度をモニタします。送信元ツリーのトラフィック速度がグループの SPT しきい値を下回っている状況が 1 分以上継続した場合、ルータはこの送信元の共有ツリーに再び切り替えようとします。

    （注） ASA は共有ツリー上のトラフィック速度を測定し、この速度とグループの SPT しきい値を 1 秒ごとに比較します。トラフィック速度が SPT しきい値を超えた場合は、トラフィック速度の次の測定が行われるまで、(*, G) エントリに J - Join SPT フラグが設定されます。共有ツリーに次のパケットが着信し、新しい測定間隔が開始されると、フラグが解除されます。

    グループにデフォルトの SPT しきい値（0 Kbps）が使用されている場合、(*, G) エントリには常に J - Join SPT フラグが設定され、解除されません。デフォルトの SPT しきい値が使用されている場合に、新しい送信元からトラフィックを受信すると、ASA は最短パス送信元ツリーにただちに切り替えます。

- **Timers:Uptime/Expires**：Uptime は、エントリが IP マルチキャスト ルーティング テーブルに格納されていた期間（時間、分、秒）をインターフェイスごとに示します。Expires は、IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）をインターフェイスごとに示します。
- **Interface state**：着信インターフェイスまたは発信インターフェイスの状態を示します。
  - **Interface**：着信インターフェイスまたは発信インターフェイスのリストに表示されるインターフェイス名。
  - **State**：アクセス リストまたは Time to Live（TTL）しきい値による制限があるかどうかに応じて、インターフェイス上で転送、プルーニング、ヌル値化のいずれの処理がパケットに対して実行されるかを示します。
- **(*, 239.1.1.40)** と **(* , 239.2.2.1)**：IP マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元の IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元の位置に置かれたアスタリスク（*）は、すべての送信元を意味します。
- **RP**：RP のアドレス。スパース モードで動作するルータおよびアクセス サーバの場合、このアドレスは常に 224.0.0.0 です。
- **Incoming interface**：送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。
- **RPF nbr**：送信元に対するアップストリーム ルータの IP アドレス。
- **Outgoing interface list**：パケット転送時に使用されるインターフェイス。

関連コマンド

コマンド	説明
clear configure mroute	実行コンフィギュレーションから **mroute** コマンドを削除します。
mroute	スタティック マルチキャスト ルートを設定します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	設定されているマルチキャスト ルートを表示します。

show nac-policy コマンド～ show ospf virtual-links コマンド

show nac-policy

NAC ポリシーの使用状況の統計およびグループ ポリシーに対する NAC ポリシーの割り当てを表示するには、特権 EXEC モードで **show nac-policy** コマンドを使用します。

show nac-policy [*nac-policy-name*]

構文の説明

nac-policy-name	(任意)使用状況の統計を表示する対象の NAC ポリシー名。

デフォルト

名前を指定しない場合は、すべての NAC ポリシー名がそれぞれの統計情報とともに CLI に一覧表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	—	• 可

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、framework1 および framework2 という名前の NAC ポリシーのデータの例を示します。

```
ciscoasa(config)# show nac-policy
nac-policy framework1 nac-framework
  applied session count = 0
```

```
  applied group-policy count = 2
  group-policy list:    GroupPolicy2    GroupPolicy1
nac-policy framework2 nac-framework is not in use.
```

各 NAC ポリシーの 1 行めは、名前とタイプ（nac-framework）を示します。ポリシーがどのグループ ポリシーにも割り当てられていない場合は、CLI のポリシー タイプの隣に「is not in use」というテキストが表示されます。それ以外は、そのグループ ポリシーの使用状況データが CLI に表示されます。表 10-1 に、**show nac-policy** コマンドのフィールドの説明を示します。

表 10-1　show nac-policy コマンドのフィールド

フィールド	説明
applied session count	この ASA が NAC ポリシーを適用した VPN セッションの累積数。
applied group-policy count	この ASA が NAC ポリシーを適用したグループ ポリシーの累積数。
group-policy list	NAC ポリシーが割り当てられているグループ ポリシーのリスト。この場合、グループ ポリシーの使用状況によってこのリストに表示されるかどうかは決まりません。NAC ポリシーが実行コンフィギュレーションのグループ ポリシーに割り当てられている場合は、このリストにグループ ポリシーが表示されます。

関連コマンド

clear nac-policy	NAC ポリシー使用状況の統計情報をリセットします。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
show vpn-session_summary.db	IPSec、Cisco WebVPN、および NAC の各セッションの数を表示します。

show nameif

nameif コマンドを使用して設定されているインターフェイス名を表示するには、特権 EXEC モードで **show nameif** コマンドを使用します。

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name* | **zone**]

構文の説明

mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
サブインターフェイス	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
zone	（オプション）ゾーン名を表示します。

デフォルト

インターフェイスを指定しない場合、ASA はすべてのインターフェイス名を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(2)	**zone** キーワードが追加されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名はコンテキスト内だけで指定できます。このコマンドの出力では、Interface カラムにはマッピング名のみが示されます。

例

次に、**show nameif** コマンドの出力例を示します。

```
ciscoasa# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

show nameif zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show nameif zone
Interface                Name                    zone-name    Security
GigabitEthernet0/0       inside-1                inside-zone    100
GigabitEthernet0/1.21    inside                  inside-zone    100
GigabitEthernet0/1.31    4                                      0
GigabitEthernet0/2       outside                 outside-zone   0
Management0/0            lan                                    0
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show nat

NAT ポリシーの統計情報を表示するには、特権 EXEC モードで **show nat** コマンドを使用します。

show nat [**interface** *name*] [*ip_addr* [*mask*] | {**object** | **object-group**} *name*]
[**translated** [**interface** *name*] {*ip_addr* [*mask*] | {**object** | **object-group**} *name*}] [**detail**]

構文の説明

detail	(任意)オブジェクト フィールドの追加詳細拡張を含めます。
interface *name*	(任意)送信元インターフェイスを指定します。
ip_addr [*mask*]	(オプション)IP アドレスおよびサブネット マスクを指定します。
object *name*	(任意)ネットワーク オブジェクトまたはサービス オブジェクトを指定します。
object-group *name*	(任意)ネットワーク オブジェクト グループを指定します。
translated	(オプション)変換されたパラメータを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.0(1)	IPv6 トラフィックのサポート、および IPv4 と IPv6 間の変換が追加されました。

使用上のガイドライン

show nat コマンドを使用して、NAT ポリシーの実行時表示を表示します。**detail** オプション キーワードを使用して、オブジェクトを拡張し、オブジェクト値を表示します。追加のセレクタ フィールドを使用して、**show nat** コマンド出力を制限することができます。

例

次に、**show nat** コマンドの出力例を示します。

```
ciscoasa# show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
```

```
   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0

ciscoasa# show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
    1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

次に、IPv6 と IPv4 間の変換が見られる **show nat detail** コマンドの出力例を示します。

```
ciscoasa# show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

次に、**show nat divert ipv6** コマンドの出力例を示します。

```
ciscoasa# show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

関連コマンド

コマンド	説明
clear nat counters	NAT ポリシー カウンタをクリアします。
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。

show nat divert-table

NAT 迂回テーブルの統計情報を表示するには、特権 EXEC モードで **show nat divert-table** コマンドを使用します。

show nat divert-table [**ipv6**] [**interface** *name*]

構文の説明

ipv6	(オプション)迂回テーブルの IPv6 エントリを表示します。
interface *name*	(オプション)指定した送信元インターフェイスに出力を限定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

show nat divert-table コマンドを使用して、NAT 迂回テーブルの実行時表現を表示します。迂回テーブルの IPv6 エントリを表示するには、**ipv6** オプション キーワードを使用します。特定の発信元インターフェイスの NAT 迂回テーブルを表示するには、**interface** オプション キーワードを使用します。

例

次に、**show nat divert-table** コマンドの出力例を示します。

```
ciscoasa# show nat divert-table
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
```

```
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad1867b0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

次に、**show nat divert ipv6** コマンドの出力例を示します。

```
ciscoasa# show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

関連コマンド

コマンド	説明
clear nat counters	NAT ポリシー カウンタをクリアします。
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。
show nat	NAT ポリシーの実行時表現を表示します。

show nat pool

NAT プールの使用状況を表示するには、特権 EXEC モードで **show nat pool** コマンドを使用します。

show nat pool

show nat pool cluster

構文の説明

クラスタ	(オプション)ASA クラスタリングがイネーブルの場合、オーナー ユニットとバックアップ ユニットへの PAT アドレスの現在の割り当てを表示します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
8.4(3)	出力が変更されて、拡張 PAT の宛先アドレスが表示されるようになりました。PAT の範囲も、**flat** キーワードと **include-reserve** キーワードの使用に応じて変更されました。
9.0(1)	IPv6 トラフィックのサポートと、PAT アドレスの所有者ユニットおよびバックアップ ユニットに対する現在の割り当てを示すための **cluster** キーワードが追加されました。

使用上のガイドライン

NAT プールは、マッピングされたプロトコル/IP アドレス/ポート範囲ごとに作成されます。デフォルトのポート範囲は、1 ー 511、512 ー 1023、および 1024 ー 65535 です。**nat** コマンドで PAT プールに対して **flat** キーワードを使用すると、範囲数が減り、範囲が大きくなります。

各 NAT プールは、最後に使用された後、少なくとも 10 分間存在します。10 分のホールドダウンタイマーは、**clear xlate** で変換をクリアするとキャンセルされます。

例

次に、**show running-config object network** コマンドによって表示される、ダイナミック PAT ルールによって作成された NAT プールの出力例を示します

```
ciscoasa(config)# show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25

ciscoasa# show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

次は、PAT プールに **flat** オプションを使用した場合の **show nat pool** コマンドの出力例です。**include-reserve** キーワードを指定しないと、2 つの範囲が示されます。低い方の範囲は、1024 未満の送信元ポートが同じポートにマッピングされているときに使用されます。

```
ciscoasa# show nat pool

ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

次は、PAT プールに **flat include-reserve** オプションを使用した場合の **show nat pool** コマンドの出力例です。

```
ciscoasa# show nat pool

ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

次は、PAT プールに **extended flat include-reserve** オプションを使用した場合の **show nat pool** コマンドの出力例です。重要な項目はカッコで囲まれたアドレスです。これらは拡張 PAT に使用される宛先アドレスです。

```
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
UDP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

関連コマンド

コマンド	説明
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。
show nat	NAT ポリシーの統計情報を表示します。

show nat proxy-arp

NAT プロキシ ARP テーブルを表示するには、特権 EXEC モードで **show nat proxy-arp** コマンドを使用します。

show nat proxy-arp [**ipv6**] [**interface** *name*]

構文の説明

ipv6	(オプション)プロキシ ARP テーブルの IPv6 エントリを表示します。
interface *name*	(オプション)指定した送信元インターフェイスに出力を限定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

NAT プロキシ ARP テーブルの実行時表現を表示するには、**show nat proxy-arp** コマンドを使用します。プロキシ ARP テーブルの IPv6 エントリを表示するには、**ipv6** オプション キーワードを使用します。特定の発信元インターフェイスの NAT プロキシ ARP テーブルを示するには、**interface** オプション キーワードを使用します。

例

次に、**show nat proxy-arp** コマンドの出力例を示します。

```
ciscoasa# show nat proxy-arp
Nat Proxy-arp Table
id=0x00007f5558bbbfc0, ip/id=10.10.1.134, mask=255.255.255.255 ifc=test2
    config:(inside) to (test2) source dynamic inside_v6 outside_v4_pat  destination
static inside_v6_nat any
id=0x00007f5558bbbfc0, ip/id=10.10.1.135, mask=255.255.255.255 ifc=test2
    config:(inside) to (test2) source dynamic inside_v6 outside_v4_pat  destination
static inside_v6_nat any
id=0x00007f55595ad2c0, ip/id=10.86.118.2, mask=255.255.255.255 ifc=inside
    config:(inside) to (test2) source dynamic inside_v6 interface  dns
id=0x00007f5559424e80, ip/id=10.100.10.1, mask=255.255.255.255 ifc=NP Identity Ifc
    config:(any) to (any) source dynamic src_network pat-pool mapped-pat-pool
```

```
id=0x00007f5559424e80, ip/id=10.100.10.2, mask=255.255.255.255 ifc=NP Identity Ifc
    config:(any) to (any) source dynamic src_network pat-pool mapped-pat-pool
id=0x00007f5544785700, ip/id=10.7.17.2, mask=255.255.255.254 ifc=NP Identity Ifc
    config:(any) to (any) source static test2 10.3.3.0
id=0x00007f554c4ae740, ip/id=10.1.1.1, mask=255.255.255.255 ifc=NP Identity Ifc
```

関連コマンド

コマンド	説明
clear nat counters	NAT ポリシー カウンタをクリアします。
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。
show nat	NAT ポリシーの実行時表現を表示します。

show ntp associations

NTP アソシエーション情報を表示するには、ユーザ EXEC モードで **show ntp associations** コマンドを使用します。

show ntp associations [**detail**]

構文の説明

detail	(任意)各アソシエーションの追加情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

出力の説明については、「例」を参照してください。

例

次に、**show ntp associations** コマンドの出力例を示します。

```
ciscoasa> show ntp associations
     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

表 10-2 に、各フィールドの説明を示します。

表 10-2　show ntp associations のフィールド

フィールド	説明
（表示行の行頭文字）	表示行の行頭には、次の文字が 1 つまたはそれ以上表示されます。 • *: このピアに同期しています。 • #: このピアに対してほぼ同期しています。 • +: ピアは同期可能な対象として選択されています。 • -: ピアが選択候補です。 • ~: ピアがスタティックに設定されていますが、同期していません。
address	NTP ピアのアドレス。
ref clock	ピアのリファレンス クロックのアドレス。
st	ピアの層。
when	ピアから最終 NTP パケットが受信されてからの時間。
poll	ポーリング間隔（秒）。
reach	ピアの到達可能性（8 進のビット ストリング）。
delay	ピアまでのラウンド トリップ遅延（ミリ秒）。
offset	ローカル クロックに対するピア クロックの相対時間（ミリ秒）。
disp	分散値。

次に、**show ntp associations detail** コマンドの出力例を示します。

```
ciscoasa> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87    0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74    0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62    16000.0
```

表 10-3 に、各フィールドの説明を示します。

表 10-3　show ntp associations detail のフィールド

フィールド	説明
IP-address configured	サーバ（ピア）の IP アドレス。
（ステータス）	• our_master: ASA がこのピアに対して同期しています。 • selected: ピアは同期可能な対象として選択されています。 • candidate: ピアが選択候補です。

表 10-3　show ntp associations detail のフィールド(続き)

フィールド	説明
(健全性)	• sane: ピアが基本健全性チェックをパスしました。 • insane: ピアが基本健全性チェックで失敗しました。
(有効性)	• valid: ピア時間は有効であると見なされています。 • invalid: ピア時間は無効であると見なされています。 • leap_add: ピアが、うるう秒が加算されることをシグナリングしています。 • leap-sub: ピアが、うるう秒が減算されることをシグナリングしています。
stratum	ピアの層。
(リファレンス ピア)	unsynced: ピアは、他のどのマシンにも同期されていません。 ref ID: ピアの同期対象となるマシンのアドレス。
time	ピアがマスターから受信した最終タイムスタンプ。
our mode client	ピアに対する相対的なモード。常に「クライアント」です。
peer mode server	サーバに相対的なピアのモード。
our poll intvl	ピアに対するポーリング間隔。
peer poll intvl	ピアからのポーリング間隔。
root delay	ルートへのパスに沿った遅延(最上位ストラタム 1 の時刻源)。
root disp	ルートへのパスの分散。
reach	ピアの到達可能性(8 進のビット ストリング)。
sync dist	ピアの同期間隔。
delay	ピアまでのラウンド トリップ遅延。
offset	クロックに相対的なピア クロックのオフセット。
dispersion	ピア クロックの分散。
precision	ピア クロックの精度(ヘルツ)。
version	ピアが使用中の NTP バージョン番号。
org time	開始時のタイムスタンプ。
rcv time	受信時のタイムスタンプ。
xmt time	送信時のタイムスタンプ。
filtdelay	各サンプルのラウンド トリップ遅延(ミリ秒)。
filtoffset	各サンプルのクロック オフセット(ミリ秒)。
filterror	各サンプルの誤差の概算値。

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。

コマンド	説明
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、ASA のキー ID を指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show ntp status

各 NTP アソシエーションのステータスを表示するには、ユーザ EXEC モードで **show ntp status** コマンドを使用します。

show ntp status

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

出力の説明については、「例」を参照してください。

例

次に、**show ntp status** コマンドの出力例を示します。

```
ciscoasa> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

表 10-4 に、各フィールドの説明を示します。

表 10-4　show ntp status のフィールド

フィールド	説明
Clock	• synchronized：ASA が NTP サーバに対して同期しています。 • unsynchronized：ASA が NTP サーバに対して同期していません。
stratum	このシステムの NTP ストラタム。
リファレンス	ASA の同期対象になる NTP サーバのアドレス。
nominal freq	システム ハードウェア クロックの公称周波数。
actual freq	システム ハードウェア クロックの測定周波数。
precision	このシステムのクロックの精度(ヘルツ)。
reference time	リファレンス タイムスタンプ。
clock offset	同期されたピアに対するシステム クロックのオフセット。
root delay	ルート クロックまでのパスに沿った合計遅延。
root dispersion	ルート パスの分散。
peer dispersion	同期されたピアの分散。

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、ASA のキー ID を指定します。
show ntp associations	ASA が関連付けられている NTP サーバを表示します。

show nve

NVE インターフェイスのパラメータ、ステータスおよび統計情報を表示するには、特権 EXEC モードで **show nve** コマンドを使用します。

show nve [1] [summary]

構文の説明

1	(オプション)NVE インスタンスを指定します。これは、常に 1 です。
summary	(オプション)NVE インターフェイスのステータス、NVE インターフェイスの背後にある VNI の数および検出された VTEP の数のみを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。

例

show nve 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show nve 1
ciscoasa(config-if)# show nve
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
```

```
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

show nve 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

show object-group

オブジェクト グループのタイプがネットワーク オブジェクトグループ タイプである場合にオブジェクト グループ情報および関連ヒット カウントを表示するには、特権 EXEC モードで **show object-group** コマンドを使用します。

show object-group [**protocol** | **service** | **icmp-type** | **id** *object_group_name*]

構文の説明

icmp-type	(任意)ICMP タイプのオブジェクト グループ。
id *object_group_name*	(オプション)オブジェクト グループを名前で特定します。
protocol	(任意)プロトコルタイプのオブジェクト グループ。
service	(任意)サービスタイプのオブジェクト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

オブジェクト グループのタイプがネットワーク オブジェクトグループ タイプである場合に、オブジェクト グループを表示しようとするルーチンでは、オブジェクト ヒットも表示されます。他のタイプのオブジェクト グループの場合、ヒット カウントは表示されません。

例

次に、「Anet」という名前のネットワーク オブジェクト グループに関する情報を表示する、**show object-group** コマンドの出力例を示します。

```
ciscoasa# show object-group id Anet
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

次に、サービス グループに関する情報を表示する、**show object-group** コマンドの出力例を示します。

```
ciscoasa (config)# show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp

   object-group protocol C-grp-proto
   protocol-object ospf
```

次に、プロトコルに関する情報を表示する、**show object-group** コマンドの出力例を示します。

```
ciscoasa (config)# show object-group protocol
object-group protocol C-grp-proto
   protocol-object ospf
```

関連コマンド

コマンド	説明
clear object-group	指定されたオブジェクト グループのネットワーク オブジェクトのヒット カウントをクリアします。
show access list	すべてのアクセス リスト、関連拡張アクセス リスト エントリ、およびヒット カウントを表示します。

show ospf

OSPF ルーティング プロセスに関する一般情報を表示するには、特権 EXEC モードで **show ospf** コマンドを使用します。

show ospf [*pid* [*area_id*]]

構文の説明

area_id	（任意）OSPF アドレス範囲に関連付けられているエリアの ID。
pid	（任意）OSPF プロセスの ID。

デフォルト

pid を指定しない場合は、すべての OSPF プロセスが一覧表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

pid を指定すると、指定したルーティング プロセスの情報のみが含まれます。

例

次に、**show ospf** コマンドの出力例を示します。ここでは、特定の OSPF ルーティング プロセスに関する一般情報を表示する例を示しています。

```
ciscoasa# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

次に、**show ospf** コマンドの出力例を示します。ここでは、すべての OSPF ルーティング プロセスに関する一般情報を表示する例を示しています。

```
ciscoasa# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0

 Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf border-routers

ABR および ASBR に対する内部 OSPF ルーティング テーブル エントリを表示するには、特権 EXEC モードで **show ospf border-routers** コマンドを使用します。

show ospf border-routers

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、**ospf border-routers** コマンドの出力例を示します。

```
ciscoasa# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf database

ASA 上の OSPF トポロジ データベースに格納されている情報を表示するには、特権 EXEC モードで **show ospf database** コマンドを使用します。

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originate** | **adv-router** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

構文の説明

addr	(任意)ルータのアドレス。
adv-router	(任意)アドバタイズされたルータ。
area_id	(任意)OSPF アドレス範囲に関連付けられているエリアの ID。
asbr-summary	(任意)ASBR リストの要約を表示します。
database	データベース情報を表示します。
database-summary	(任意)データベース全体の要約リストを表示します。
external	(任意)指定した自律システムの外部のルートを表示します。
internal	(任意)指定した自律システム内部のルート。
lsid	(任意)LSA ID。
network	(任意)ネットワークに関する OSPF データベース情報を表示します。
nssa-external	(任意)外部の Not-So-Stubby Area リストを表示します。
pid	(任意)OSPF プロセスの ID。
ルータ	(任意)ルータを表示します。
self-originate	(任意)指定した自律システムに関する情報を表示します。
summary	(任意)リストの要約を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、ASA 上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

例

次に、**show ospf database** コマンドの出力例を示します。

```
ciscoasa# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

次に、**show ospf database asbr-summary** コマンドの出力例を示します。

```
ciscoasa# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

次に、**show ospf database router** コマンドの出力例を示します。

```
ciscoasa# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
```

```
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

次に、**show ospf database network** コマンドの出力例を示します。

```
ciscoasa# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

次に、**show ospf database summary** コマンドの出力例を示します。

```
ciscoasa# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

次に、**show ospf database external** コマンドの出力例を示します。

```
ciscoasa# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf events

OSPF 内部イベント情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ospf events** コマンドを使用します。

show ospf [*process_id*] **events** [*type*]

構文の説明

process_id	（オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
type	（オプション）表示するイベント タイプのリスト。タイプを 1 つ以上指定しないと、すべてのイベントが表示されます。次のタイプでフィルタリングできます。 • **generic**：一般的なイベント。 • **interface**：インターフェイス状態変化イベント。 • **lsa**：LSA 到着イベントおよび LSA 生成イベント。 • **neighbor**：ネイバー状態変化イベント。 • **reverse**：逆の順序でイベントを表示。 • **rib**：ルータ情報ベースの更新イベント、削除イベント、および再配布イベント。 • **spf**：SPF のスケジューリング イベントおよび SPF 実行イベント。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—
ユーザ EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、**show ospf events** コマンドの出力例を示します。

```
ciscoasa# show ospf events

            OSPF Router with ID (192.168.77.1) (Process ID 5)

   1 Apr 27 16:33:23.556: RIB Redist, dest 0.0.0.0, mask 0.0.0.0, Up
   2 Apr 27 16:33:23.556: Rescanning RIB:  0x00x0
   3 Apr 27 16:33:23.556: Service Redist scan:  0x00x0
```

関連コマンド

コマンド	説明
show ospf	OSPF ルーティング プロセスのすべての設定を表示します。
show ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）への内部 OSPF ルーティング テーブル エントリを表示します。

show ospf flood-list

インターフェイスを介してフラッディングされるのを待機している OSPF LSA のリストを表示するには、特権 EXEC モードで **show ospf flood-list** コマンドを使用します。

show ospf flood-list *interface_name*

構文の説明

interface_name	ネイバー情報を表示するインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、ASA 上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

例

次に、**show ospf flood-list** コマンドの出力例を示します。

```
ciscoasa# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf interface

OSPF 関連のインターフェイス情報を表示するには、特権 EXEC モードで **show ospf interface** コマンドを使用します。

show ospf interface [*interface_name*]

構文の説明

interface_name	（任意）OSPF 関連の情報を表示するインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

interface_name 引数を指定せずに使用すると、すべてのインターフェイスの OSPF 情報が表示されます。

例

次に、**show ospf interface** コマンドの出力例を示します。

```
ciscoasa# show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

show ospf neighbor

インターフェイスごとの OSPF ネイバー情報を表示するには、特権 EXEC モードで **show ospf neighbor** コマンドを使用します。

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

構文の説明

detail	（任意）指定したルータに関する詳細な情報を表示します。
interface_name	（任意）ネイバー情報を表示するインターフェイスの名前。
nbr_router_id	（任意）ネイバー ルータのルータ ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、**show ospf neighbor** コマンドの出力例を示します。ここでは、インターフェイスごとの OSPF ネイバー情報を表示する例を示しています。

```
ciscoasa# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

次に、**show ospf neighbor detail** コマンドの出力例を示します。指定された OSPF ネイバーの詳細情報を表示する方法を示します。

```
ciscoasa# show ospf neighbor detail

Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
    Neighbor priority is 1, State is FULL, 46 state changes
    DR is 15.1.1.62 BDR is 15.1.1.60
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
    Dead timer due in 0:00:24
    Neighbor is up for 01:42:15
    Index 5/5, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

関連コマンド

コマンド	説明
neighbor	非ブロードキャスト ネットワークに相互接続する OSPF ルータを設定します。
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf nsf

OSPFv2 関連の NSF 情報を表示するには、特権 EXEC モードで **show ospf nsf** コマンドを使用します。

show ospf nsf

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

例

次に、**show ospf nsf** コマンドの出力例を示します。

```
ciscoasa# show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
    Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
    OSPF restart state is
    Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
    Config wait timer interval 10, timer not running
    Dbase wait timer interval 120, timer not running
```

関連コマンド

コマンド	説明
nsf cisco	NSF 対応ルータの Cisco NSF をイネーブルにします。
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf request-list

ルータによって要求されたすべての LSA のリストを表示するには、特権 EXEC モードで **show ospf request-list** コマンドを使用します。

show ospf request-list *nbr_router_id interface_name*

構文の説明

interface_name	ネイバー情報を表示するインターフェイスの名前。このインターフェイスからルータによって要求されたすべての LSA のリストを表示します。
nbr_router_id	ネイバー ルータのルータ ID。このネイバーからルータによって要求されたすべての LSA のリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、**show ospf request-list** コマンドの出力例を示します。

```
ciscoasa# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

関連コマンド

コマンド	説明
show ospf retransmission-list	再送信を待機しているすべての LSA のリストを表示します。

show ospf retransmission-list

再送信されるのを待機しているすべての LSA のリストを表示するには、特権 EXEC モードで **show ospf retransmission-list** コマンドを使用します。

show ospf retransmission-list *nbr_router_id interface_name*

構文の説明

interface_name	ネイバー情報を表示するインターフェイスの名前。
nbr_router_id	ネイバー ルータのルータ ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、ASA 上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

nbr_router_id 引数を指定すると、このネイバーの、再送信されるのを待機しているすべての LSA のリストが表示されます。

interface_name 引数を指定すると、このインターフェイスの、再送信されるのを待機しているすべての LSA のリストが表示されます。

例

次に、**show ospf retransmission-list** コマンドの例を示します。例では、*nbr_router_id* 引数は 192.168.1.11 で、*if_name* 引数は outside です。

```
ciscoasa# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2
```

```
Type   LS ID           ADV RTR        Seq NO       Age   Checksum
   1   192.168.1.12    192.168.1.12   0x80000210   0     0xB196
```

関連コマンド

コマンド	説明
show ospf request-list	ルータによって要求されたすべての LSA のリストを表示します。

show ospf rib

OSPF ルータ情報ベース（RIB）を表示するには、特権 EXEC モードで **show ospf rib** コマンドを使用します。

show ospf [*pid* [*area_id*]] **rib** [*network_prefix* [*network_mask*] | **detail** | **redistribution** [*network_prefix* [*network_mask*] | **detail**]]

構文の説明

area_id	（任意）OSPF アドレス範囲に関連付けられているエリアの ID。
pid	（任意）OSPF プロセスの ID。
network_prefix [*network_mask*]	（オプション）表示するルータのネットワーク プレフィックスおよびオプションでマスク。次に例を示します。 10.100.10.1 10.100.10.0 255.255.255.0
detail	（オプション）RIB に関する詳細情報を表示します。
再配布	（オプション）再配布情報を表示します。ネットワーク プレフィックスとマスクを指定するか、または redistribution キーワードの後ろに **detail** キーワードを指定することもできます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

show ospf statistics

さまざまな OSPF 統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ospf statistics** コマンドを使用します。

show ospf [*process_id*] **statistics** [**detail**]

構文の説明

detail	(オプション) トリガー ポイントを含む詳細な SPF 情報を指定します。
process_id	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—
ユーザ EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

SPF が実行された回数、原因、および期間を表示するには、このコマンドを使用します。

例

次に、**show ospf statistics** コマンドの出力例を示します。

```
ciscoasa# show ospf 10 statistics detail


Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
```

```
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

関連コマンド

コマンド	説明
show ospf	OSPF ルーティング プロセスのすべての設定を表示します。
show ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）への内部 OSPF ルーティング テーブル エントリを表示します。

show ospf summary-address

OSPF プロセスに対して設定されたすべてのサマリー アドレス再配布情報のリストを表示するには、特権 EXEC モードで **show ospf summary-address** コマンドを使用します。

show ospf summary-address

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、**show ospf summary-address** コマンドの出力例を示します。この例は、ID が 5 である OSPF プロセスに対してサマリー アドレスが設定される前に、すべてのサマリー アドレス再配布情報のリストを表示する方法を示しています。

```
ciscoasa# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

関連コマンド

コマンド	説明
summary-address	OSPF の集約アドレスを作成します。

show ospf traffic

特定の OSPF インスタンスによって処理（送信または受信）されたパケットのさまざまなタイプのリストを表示するには、特権 EXEC モードで **show ospf traffic** コマンドを使用します。このコマンドを使用すると、デバッグを有効にすることなく、処理されるさまざまなタイプの OSPF パケットのスナップショットを取得できます。設定された 2 つの OSPF インスタンスがある場合、show ospf traffic コマンドは、各インスタンスのプロセス ID とともに、両方のインスタンスの統計情報を表示します。また、**show ospf** *process_id* **traffic** コマンドを使用して、シングル インスタンスの統計情報を表示することもできます。

show ospf traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、デバッグを有効にすることなく、処理されるさまざまなタイプの OSPF パケットのスナップショットを取得できます。設定された 2 つの OSPF インスタンスがある場合、**show ospf traffic** コマンドは、各インスタンスのプロセス ID とともに、両方のインスタンスの統計情報を表示します。また、**show ospf** *process_id* **traffic** コマンドを使用して、シングル インスタンスの統計情報を表示することもできます。

例

次に、**show ospf traffic** コマンドの出力例を示します。

```
ciscoasa# show ospf traffic

OSPF statistics (Process ID 70):

       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

```
Sent: 485 total
      472 hello, 7 database desc, 1 link state req
      3 link state updates, 2 link state acks
```

関連コマンド

コマンド	説明
show ospf virtual-links	OSPF 仮想リンクのパラメータと現在の状態を表示します。

show ospf virtual-links

OSPF 仮想リンクのパラメータと現在の状態を表示するには、特権 EXEC モードで **show ospf virtual-links** コマンドを使用します。

show ospf virtual-links

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、**show ospf virtual-links** コマンドの出力例を示します。

```
ciscoasa# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

関連コマンド

コマンド	説明
area virtual-link	OSPF 仮想リンクを定義します。

show pager コマンド～ show route コマンド

show pager

インターフェイスのデフォルト ルートまたはスタティック ルートを表示するには、特権 EXEC モードで **show pager** コマンドを使用します。

show pager

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

例

次に、**show pager** コマンドの出力例を示します。

```
ciscoasa(config)# show pager
pager lines 0
```

関連コマンド

コマンド	説明
clear configure pager	Telnet セッションで「---More---」プロンプトまでに表示されるよう設定されている行数を実行コンフィギュレーションから削除します。
show running-config pager	実行コンフィギュレーションに Telnet セッションで「---More---」プロンプトまでに表示されるよう設定されている行数を表示します。
terminal pager	Telnet セッションで「---More---」プロンプトまでに表示する行数を設定します。このコマンドは実行コンフィギュレーションに保存されません。

show password encryption

パスワード暗号化のコンフィギュレーション設定を表示するには、特権 EXEC モードで **show password encryption** コマンドを使用します。

show password encryption

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
8.4(1)	ユーザ コンテキストに show password encryption が追加されました。

使用上のガイドライン

キーが **write memory** コマンドを使用して保存されている場合、キー ハッシュの横に「saved」が表示されます。キーがない場合、またはキーが実行コンフィギュレーションから削除された場合、ハッシュ値の代わりに「Not set」が表示されます。

例

次に、**show password encryption** コマンドの出力例を示します。

```
ciscoasa# show password encryption
Password Encryption: Enabled
Master key hash: 0x35859e5e 0xc607399b 0x35a3438f 0x55474935 0xbec1ee7d(not saved)
```

関連コマンド

コマンド	説明
password encryption aes	パスワードの暗号化をイネーブルにします。
key config-key password-encrypt	暗号キーを生成するために使用されるパス フレーズを設定します。

show perfmon

ASA のパフォーマンスに関する情報を表示するには、特権 EXEC モードで **show perfmon** コマンドを使用します。

show perfmon [**detail**]

構文の説明

detail	（任意）追加の統計情報を表示します。これらの統計情報は Cisco Unified Firewall MIB のグローバル接続オブジェクトとプロトコルごとの接続オブジェクトにより収集された情報と一致します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	ASA でこのコマンドのサポートが追加されました。
7.2(1)	**detail** キーワードが追加されました。

使用上のガイドライン

このコマンドの出力は、Telnet セッションには表示されません。

perfmon コマンドでは、指定した間隔でパフォーマンス統計情報が連続的に表示されます。**show perfmon** コマンドを使用すると、すぐに情報を表示できます。

例

次に、**show perfmon** コマンドの出力例を示します。

```
ciscoasa(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
```

```
HTTP Fixup           0/s           0/s
FTP Fixup            0/s           0/s
AAA Authen           0/s           0/s
AAA Author           0/s           0/s
AAA Account          0/s           0/s
```

次に、**show perfmon detail** コマンドの出力例を示します。

```
ciscoasa(config)# show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s           0/s
Connections          0/s           0/s
TCP Conns            0/s           0/s
UDP Conns            0/s           0/s
URL Access           0/s           0/s
URL Server Req       0/s           0/s
TCP Fixup            0/s           0/s
HTTP Fixup           0/s           0/s
FTP Fixup            0/s           0/s
AAA Authen           0/s           0/s
AAA Author           0/s           0/s
AAA Account          0/s           0/s
TCP Intercept        0/s           0/s

SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

関連コマンド

コマンド	説明
perfmon	指定した間隔で詳細なパフォーマンス モニタ情報を表示します。

show phone-proxy（廃止予定）

phone-proxy 固有の情報を表示するには、グローバル コンフィギュレーション モードで **show phone-proxy** コマンドを使用します。

show phone-proxy [media-sessions [detail] | signaling-sessions [detai] | secure-phones]

構文の説明

detail	詳細情報を表示します。
media-sessions	電話プロキシによって保存されている、対応するメディア セッションを表示します。また、メディア セッションが確立されているインターフェイスに設定されているメディア ターミネーション アドレスを表示します。
secure-phones	データベースに格納されているセキュア モードに対応した電話を表示します。
signaling-sessions	電話プロキシに保存されている、対応するシグナリング セッションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
8.2(1)	コマンドが更新され、**media-sessions** キーワードを指定しても、メディア セッションが確立されているインターフェイスに設定されたメディア ターミネーション アドレスが表示されるようになりました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

例

次に、**show phone proxy** コマンドを使用して電話プロキシ固有の情報を表示する例を示します。

```
ciscoasa(config)# show phone-proxy
Phone-Proxy 'mypp': Runtime Proxy ref_cnt 2
Cluster Mode: nonsecure
Run-time proxies:
```

```
Proxy 0xd55f6fd8: Class-map: secsip, Inspect: sip
Proxy 0xd58a93a8: Class-map: secsccp, Inspect: skinny
phoneproxy(config)# show phone-proxy secure-phones
mypp: 5 in use, 5 most used
Interface  IP Address     Port  MAC            Timeout Idle
outside    69.181.112.219 10889 001e.7ac4.da9c 0:05:00 0:01:36
outside    98.208.25.87   14159 001c.581c.0663 0:05:00 0:00:04
outside    98.208.25.87   14158 0007.0e36.4804 0:05:00 0:00:13
outside    98.208.25.87   14157 001e.7ac4.deb8 0:05:00 0:00:21
outside    128.107.254.69 49875 001b.0cad.1f69 0:05:00 0:00:04
ciscoasa(config)#
```

次に、**show phone proxy** コマンドを使用して、データベースに保存されている、セキュア モードに対応した電話を表示します。

```
ciscoasa(config)# show phone-proxy secure-phones
asa_phone_proxy: 3 in use, 4 most used

Interface/IP Address      MAC               Timeout    Idle
------------------------  ----------        ---------  ------
outside:69.181.112.219    001e.7ac4.da9c    0:05:00    0:00:16
outside:69.181.112.219    0002.b9eb.0aad    0:05:00    0:00:58
outside:98.208.49.30      0007.0e36.4804    0:05:00    0:00:09
ciscoasa(config)#
```

次に、**show phone proxy** コマンドを使用して、正常に完了したコールの出力と、メディア セッションが確立されているインターフェイスに設定されたメディア ターミネーション アドレスを表示する例を示します。

```
ciscoasa(config)# show phone-proxy media-sessions
Media-session: 128.106.254.3/1168 refcnt 6
  <---> RTP connection to 192.168.200.106/25038 tx_pkts 485 rx_pkts 491
Media-session: 128.106.254.3/1170 refcnt 6
  <---> SRTP connection to 98.208.25.87/1030 tx_pkts 484 rx_pkts 485
```

関連コマンド

コマンド	説明
debug phone-proxy	電話プロキシ インスタンスからのデバッグ メッセージを表示します。
phone proxy	Phone Proxy インスタンスを設定します。

show pim bsr-router

ブートストラップ ルータ（BSR）情報を表示するには、**show pim bsr-router** コマンドを使用します。

show pim bsr-router

構文の説明

引数または変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

例

次に、**show pim bsr-router** コマンドの出力例を示します。

```
ciscoasa# show pim bsr-router
PIMv2 Bootstrap information
This system is a candidate BSR
  Candidate BSR interface GigabitEthernet0/0 is down - BSR messages not originated
  Candidate RP: 4.4.4.1(GigabitEthernet0/0), GigabitEthernet0/0 is down - not advertised
```

show pim df

ランデブー ポイント（RP）またはインターフェイスについて、双方向 DF の「勝者」を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim df** コマンドを使用します。

show pim df [**winner**] [*rp_address* | *if_name*]

構文の説明

rp_address	次のいずれか 1 つを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
if_name	インターフェイスの物理名または論理名。
winner	（任意）DF 選出の勝者をインターフェイスごと、RP ごとに表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、RP への勝者のメトリックも表示します。

例

次に、**show pim df** コマンドの出力例を示します。

```
ciscoasa# show pim df
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
```

```
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

グループ/プロトコル マッピング テーブルを表示するには、特権 EXEC モードで **show pim group-map** コマンドを使用します。

show pim group-map [**info-source**] [*group*]

構文の説明

group	(任意)次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、**ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
info-source	(任意)グループ範囲情報の情報源を表示します。
rp-timers	(オプション)グループから RP へのマッピングのアップタイムと有効期限タイマーが表示されます。

デフォルト

すべてのグループについて、グループからプロトコルへのマッピングを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは変更され、rp-timers 変数が組み込まれました。

使用上のガイドライン

このコマンドは、RP について、グループとプロトコルとのアドレス マッピングをすべて表示します。マッピングは、ASA 上でさまざまなクライアントから学習されます。

ASA の PIM 実装は、さまざまな特殊エントリをマッピング テーブルで保持しています。Auto-rp グループ範囲は、スパース モード グループ範囲から明確に拒否されます。SSM グループ範囲もスパース モードには入りません。リンクローカル マルチキャスト グループ(224.0.0.0 ～ 224.0.0.225。224.0.0.0/24 として定義)も、スパース モード グループ範囲から拒否されます。最後のエントリは、所定の RP でスパース モードに入っている残りすべてのグループを示します。

pim rp-address コマンドで複数の RP を設定した場合は、適切なグループ範囲が対応する RP とともに表示されます。グループに選択した RP を表示するには、**show pim group-map** コマンドでグループ アドレスまたは名前を指定します。

例

次に、**show pim group-map** コマンドの出力例を示します。

```
ciscoasa# show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

1 行めと 2 行めで、Auto-RP グループ範囲がスパース モード グループ範囲から明確に拒否されています。

3 行めでは、リンク ローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.255。224.0.0.0/24 として定義）もスパース モード グループ範囲から拒否されています。

4 行めでは、PIM 送信元特定マルチキャスト（PIM-SSM）グループ範囲が 232.0.0.0/8 にマッピングされています。

最後のエントリは、残りすべてのグループがスパース モードに入って、RP 10.10.3.2 にマッピングされたことを示しています。

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャスト ルーティングをイネーブルにします。
pim rp-address	PIM ランデブー ポイント（RP）のアドレスを設定します。

show pim interface

PIM に関するインターフェイス固有の情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim interface** コマンドを使用します。

show pim interface [*if_name* | **state-off** | **state-on**]

構文の説明

if_name	（任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。
state-off	（任意）PIM がディセーブルになっているインターフェイスを表示します。
state-on	（任意）PIM がイネーブルになっているインターフェイスを表示します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスに関する PIM 情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA の PIM 実装は、ASA 自体を PIM ネイバーと見なします。したがって、このコマンドの出力にあるネイバー数カラムでは、ネイバー数が実際の数よりも 1 つ多く表示されます。

例

次に、内部インターフェイスに関する PIM 情報を表示する例を示します。

```
ciscoasa# show pim interface inside
Address     Interface      Ver/     Nbr     Query      DR     DR
                           Mode     Count   Intvl      Prior
172.16.1.4 inside          v2/S     2       100 ms     1      172.16.1.4
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャスト ルーティングをイネーブルにします。

show pim join-prune statistic

PIM の加入とプルーニングに関する集約的な統計情報を表示するには、ユーザ EXEC モードと特権 EXEC モードで **show pim join-prune statistics** コマンドを使用します。

show pim join-prune statistics [*if_name*]

構文の説明

if_name	（任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて、加入とプルーニングに関する統計情報が表示されます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォールモード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

PIM の加入とプルーニングに関する統計情報をクリアするには、**clear pim counters** コマンドを使用します。

例

次に、**show pim join-prune statistic** コマンドの出力例を示します。

```
ciscoasa# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

            inside   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
         Ethernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet3   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet2   0 /    0 /    0         0 /    0 /    0
```

関連コマンド

コマンド	説明
clear pim counters	PIM トラフィック カウンタをクリアします。

show pim neighbor

PIM ネイバー テーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim neighbor** コマンドを使用します。

show pim neighbor [**count** | **detail**] [*interface*]

構文の説明

interface	（任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。
count	（任意）PIM ネイバーの合計数、および各インターフェイスの PIM ネイバーの数を表示します。
detail	（任意）upstream-detection hello オプションを通じて学習した、ネイバーの追加アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、このルータが PIM の hello メッセージを通じて学習した PIM ネイバーを特定するために使用します。また、このコマンドは、インターフェイスが指定ルータ（DR）であること、およびネイバーで双方向処理が可能になるタイミングも示します。

ASA の PIM 実装は、ASA 自体を PIM ネイバーと見なします。したがって、ASA インターフェイスがこのコマンドの出力に表示されます。ASA の IP アドレスは、アドレスの次にアスタリスク（*）を付けて示されています。

例

次に、**show pim neighbor** コマンドの出力例を示します。

```
ciscoasa# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャスト ルーティングをイネーブルにします。

show pim range-list

PIM の範囲リストの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim range-list** コマンドを使用します。

show pim range-list [*rp_address*]

構文の説明

rp_address	次のいずれか 1 つを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、マルチキャスト転送モードからグループへのマッピングを特定するために使用されます。出力には、この範囲のランデブー ポイント（RP）のアドレスも示されます（該当する場合）。

例

次に、**show pim range-list** コマンドの出力例を示します。

```
ciscoasa# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
```

```
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

関連コマンド

コマンド	説明
show pim group-map	グループから PIM モードへのマッピング、およびアクティブな RP の情報を表示します。

show pim topology

PIM トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology** コマンドを使用します。

show pim topology [*group*] [*source*]

構文の説明

group	(任意)次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、**ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
source	(任意)次のいずれかを指定できます。 • マルチキャスト送信元の名前。DNS の hosts テーブルに定義されているものか、**ipv4 host** コマンドで定義したものです。 • マルチキャスト送信元の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。

デフォルト

すべてのグループと送信元のトポロジ情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

PIM トポロジ テーブルは、所定のグループのさまざまなエントリ、(*, G)、(S, G)、(S, G)RPT をそれぞれのインターフェイス リストとともに表示するために使用します。

PIM は、これらのエントリの内容を MRIB を通じてやり取りします。MRIB は、PIM などのマルチキャスト ルーティング プロトコルと、インターネット グループ管理プロトコル(IGMP)などのローカル メンバーシップ プロトコルとの通信における仲介手段であり、システムのマルチキャスト転送エンジンです。

MRIB は、所定の (S, G) エントリについて、どのインターフェイスでデータ パケットを受け取る必要があるか、どのインターフェイスでデータ パケットを転送する必要があるかを示します。また、転送時にはマルチキャスト転送情報ベース（MFIB）テーブルを使用して、パケットごとの転送アクションを決定します。

(注) 転送情報を表示するには、**show mfib route** コマンドを使用します。

例

次に、**show pim topology** コマンドの出力例を示します。

```
ciscoasa# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルを表示します。
show pim topology reserved	予約済みグループの PIM トポロジ テーブルの情報を表示します。

show pim topology reserved

予約済みグループに関する PIM トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology reserved** コマンドを使用します。

show pim topology reserved

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show pim topology reserved** コマンドの出力例を示します。

```
ciscoasa# show pim topology reserved

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside             00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside              00:00:48  off II
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show pim topology route-count

PIM トポロジ テーブルのエントリの数を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology** コマンドを使用します。

show pim topology route-count [**detail**]

構文の説明

detail	（任意）グループごとに、数に関する詳細な情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルのエントリの数を表示します。エントリに関する詳細な情報を表示するには、**show pim topology** コマンドを使用します。

例

次に、**show pim topology route-count** コマンドの出力例を示します。

```
ciscoasa# show pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show pim traffic

PIM トラフィックのカウンタを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim traffic** コマンドを使用します。

show pim traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

PIM トラフィックのカウンタをクリアするには、**clear pim counters** コマンドを使用します。

例

次に、**show pim traffic** コマンドの出力例を示します。

```
ciscoasa# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                  Received     Sent
Valid PIM Packets                        0        9485
Hello                                    0        9485
Join-Prune                               0           0
Register                                 0           0
Register Stop                            0           0
Assert                                   0           0
Bidir DF Election                        0           0
```

```
Errors:
Malformed Packets                                   0
Bad Checksums                                       0
Send Errors                                         0
Packet Sent on Loopback Errors                      0
Packets Received on PIM-disabled Interface          0
Packets Received with Unknown PIM Version           0
```

関連コマンド

コマンド	説明
clear pim counters	PIM トラフィック カウンタをクリアします。

show pim tunnel

PIM トンネル インターフェイスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim tunnel** コマンドを使用します。

show pim tunnel [*if_name*]

構文の説明

if_name	(任意)インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて PIM トンネル情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

PIM レジスタ パケットは、仮想カプセル化トンネル インターフェイスを経由して、送信元の最初のホップ DR ルータから RP に送信されます。RP では、仮想カプセル化解除トンネルを使用して、PIM レジスタ パケットの受信インターフェイスを表現します。このコマンドは、両方のタイプのインターフェイスについてトンネル情報を表示します。

レジスタ トンネルは、(PIM レジスタ メッセージ内に)カプセル化された、送信元からのマルチキャスト パケットです。送信元は、共有ツリーを経由して、配布のために RP に送信されます。登録が適用されるのは、SM に対してのみです。SSM および双方向 PIM には適用されません。

例

次に、**show pim tunnel** コマンドの出力例を示します。

```
ciscoasa# show pim tunnel

Interface     RP Address Source Address

Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show policy-list

設定されたポリシー リストとポリシー リストのエントリに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show policy-list** コマンドを使用します。

show policy-list [*policy_list_name*]

構文の説明

policy_list_name	(オプション)指定されたポリシー リストに関する情報を表示します。

デフォルト

ポリシー リストの名前を指定しない場合、このコマンドはすべてのポリシー リストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ルート マップの一致基準として BGP ルーティングにポリシー リストを使用します。

例

次に、**show policy-list** コマンドの出力例を示します。

```
ciscoasa# show policy-list

policy-list policy_list_2 permit
  Match clauses:
    ip address prefix-lists: prefix_1

policy-list policy_list_1 permit
  Match clauses:
    ip address (access-lists): test
    interface inside
```

関連コマンド

コマンド	説明
policy-list	ポリシー リストを設定します。

show policy-route

ポリシーベースのルーティング設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show policy-route** コマンドを使用します。

show policy-route

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

例

次に、**show policy-list** コマンドの出力例を示します。

```
ciscoasa# show policy-route
Interface            Route map
GigabitEthernet0/0   equal-access
```

関連コマンド

コマンド	説明
policy-route	ポリシーベース ルーティングを設定します。

show port-channel

EtherChannel 情報を詳細な 1 行のサマリー形式で表示する場合、またはポートとポートチャネルの情報を表示する場合は、特権 EXEC モードで **show port-channel** コマンドを使用します。

show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

構文の説明

brief	（デフォルト）短い情報を表示します。
channel_group_number	（オプション）EtherChannel チャネル グループ番号を 1 ～ 48 の範囲で指定して、このチャネル グループに関する情報だけを表示します。
detail	（オプション）詳細な情報を表示します。
port	（オプション）各インターフェイスの情報を表示します。
protocol	（オプション）イネーブルにした場合、LACP などの EtherChannel プロトコルを表示します。
summary	（オプション）ポートチャネルの要約を表示します。

コマンド デフォルト

デフォルトは **brief** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

例

次に、**show port-channel** コマンドの出力例を示します。

```
ciscoasa# show port-channel
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

次に、**show port-channel summary** コマンドの出力例を示します。

```
ciscoasa# show port-channel summary

Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

次に、**show port-channel detail** コマンドの出力例を示します。

```
ciscoasa# show port-channel detail
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
        Ports in the group:
        -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d


Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d
```

```
Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d


Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

次に、**show port-channel port** コマンドの出力例を示します。

```
ciscoasa# show port-channel port
       Channel-group listing:
       ----------------------

Group: 1
----------
       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d


Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
```

```
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x0       0x1      0x303       0x3d


Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x0       0x1      0x302       0x3d
```

次に、**show port-channel protocol** コマンドの出力例を示します。

```
ciscoasa# show port-channel protocol
        Channel-group listing:
        ----------------------

Group: 1
----------
Protocol: LACP
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。

コマンド	説明
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）を表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

show port-channel load-balance

EtherChannel で、現在のポートチャネル ロードバランス アルゴリズムを表示する場合、また任意で特定のパラメータ セットに選択されたメンバー インターフェイスを表示する場合は、特権 EXEC モードでこのコマンドを入力します。

show port-channel *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **mac** | **l4port** | **mixed** | **vlan-only** *number*} *parameters*]

構文の説明

channel_group_number	EtherChannel チャネル グループ番号を 1 ～ 48 の範囲で指定します。
hash-result	（オプション）現在のロード バランシング アルゴリズムに入力した値をハッシュした後で選択されたメンバー インターフェイスを表示します。
ip	（オプション）IPv4 パケット パラメータを指定します。
ipv6	（オプション）IPv6 パケット パラメータを指定します。
l4port	（オプション）ポート パケット パラメータを指定します。
mac	（オプション）MAC アドレス パケット パラメータを指定します。
mixed	（オプション）IP または IPv6 パラメータの組み合わせを、ポートまたは VLAN ID（あるいはその両方）とともに指定します。
パラメータ	（オプション）パケット パラメータ。タイプによって異なります。たとえば、**ip** の場合、送信元 IP アドレス、宛先 IP アドレス、または VLAN ID（あるいはそれらの組み合わせ）を指定できます。
vlan-only	（オプション）パケットの VLAN ID を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、ASA はパケットの送信元および宛先 IP アドレス（**src-dst-ip**）に従ってインターフェイスでのパケットの負荷を分散します。アルゴリズムを変更するには、**port-channel load-balance** コマンドを参照してください。

このコマンドでは、現在のロード バランシング アルゴリズムを表示できますが、**hash-result** キーワードを使用すると、さらに、特定のパラメータを含むパケットに対してどのメンバー インターフェイスが選択されるかをテストできます。このコマンドでテストできるのは、現在のロード バランシング アルゴリズムに対してだけです。たとえば、アルゴリズムが src-dst-ip の場合は、IPv4 または IPv6 の送信元 IP アドレスおよび宛先 IP アドレスを入力します。現在のアルゴリズムで使用されていない他の引数を入力した場合、それらの引数は無視され、アルゴリズムで実際に使用されている未入力の値が 0 にデフォルト設定されます。たとえば、アルゴリズムが vlan-src-ip の場合、次のように入力します。

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

次のように入力した場合、vlan-src-ip アルゴリズムでは送信元 IP アドレス 0.0.0.0 および VLAN 0 が想定され、入力した値は無視されます。

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

例

次に、**show port-channel 1 load-balance** コマンドの出力例を示します。

```
ciscoasa# show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

次に、**show port-channel 1 load-balance hash-result** コマンドの出力例を示します。ここでは、入力したパラメータが現在のアルゴリズム（src-dst-ip）と一致しています。

```
ciscoasa# show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination
10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

次に、**show port-channel 1 load-balance hash-result** コマンドの出力例を示します。ここでは、入力したパラメータが現在のアルゴリズム（src-dst-ip）と一致しておらず、ハッシュでは 0 の値が使用されます。

```
ciscoasa# show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。

コマンド	説明
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。

show power inline

PoE インターフェイスを持つモデルの場合、インターフェイスの電源の状態を表示するには、ユーザ EXEC モードで **show power inline** コマンドを使用します。

show power inline

(注) Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

PoE インターフェイスを使用して、IP フォンまたはワイヤレス アクセス ポイントなどの電源を必要するデバイスを接続します。Firepower 1010 の場合、イーサネット 1/7 および 1/8 で PoE+ をサポートしています。ASA 5505 では、イーサネット 0/6 および 0/7 で PoE をサポートしています。

例

次に、Firepower 1010 での **show power inline** コマンドの出力例を示します。

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

次に、ASA 5505 での **show power inline** コマンドの出力例を示します。

```
ciscoasa# show power inline

  Interface     Power   Device
  -----------   -----   ------
  Ethernet0/0    n/a    n/a
  Ethernet0/1    n/a    n/a
  Ethernet0/2    n/a    n/a
  Ethernet0/3    n/a    n/a
  Ethernet0/4    n/a    n/a
  Ethernet0/5    n/a    n/a
  Ethernet0/6    On     Cisco
  Ethernet0/7    Off    n/a
```

表 11-1 に、各フィールドの説明を示します。

表 11-1　show power inline のフィールド

フィールド	説明
Interface	ASA 上のすべてのインターフェイスを表示します。PoE が使用できないインターフェイスも含みます。
電源	電源が On か Off かを示します。デバイスに電源が必要でない場合、インターフェイスにデバイスがない場合、またはインターフェイスがシャットダウンしている場合、値は Off になります。インターフェイスが PoE をサポートしていない場合、値は n/a です。
デバイス	(ASA 5505) 給電されるデバイスのタイプを表示します。Cisco または IEEE のいずれかです。デバイスが給電されていない場合、値は n/a です。デバイスの給電が Cisco の場合、ディスプレイには Cisco と表示されます。IEEE は、デバイスの給電が IEEE 802.3af 準拠であることを示します。
クラス	(Firepower 1010) 接続されているデバイスの PoE クラスを表示します。
電流 (mA)	(Firepower 1010) 使用中の電流を表示します。
電圧 (V)	(Firepower 1010) 使用中の電圧を表示します。

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
clear interface	**show interface** コマンドのカウンタをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
power inline	PoE を有効または無効にします。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show prefix-list

設定されたプレフィックス リストに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show prefix-list** コマンドを使用します。

show prefix-list [**summary** | **detail**] [*policy_list_name* [**seq** *sequence_number* | *network/length* [**longer** | **first-match**]]]

構文の説明

policy_list_name	(オプション)指定されたポリシー リストに関する情報を表示します。
summary	(オプション)要約された追加統計情報を表示します。
detail	(オプション)要約された追加統計情報とプレフィックス リストのエントリを表示します。
seq *sequence_number*	(オプション)指定されたプレフィックス リストに指定されたシーケンス番号を持つプレフィックス リストのエントリだけを表示します。
network/length [**longer** | **first-match**]	(オプション)このネットワーク アドレスおよびネットマスク長(ビット単位)を使用する、指定したプレフィックス リストのすべてのエントリを表示します。ネットワーク マスクの長さは 0 ～ 32 です。 次のキーワードを追加することで、一致条件を変更できます。 • **longer**:指定された network/length と一致するか、または(より限定的な)指定されたプレフィックス リストのエントリすべてを表示します。 • **first-match**:指定された network/length と一致する、指定されたプレフィックス リストの最初のエントリを表示します。

デフォルト

プレフィックス リストの名前を指定しない場合、このコマンドはすべてのプレフィックス リストを表示します。他のキーワードを含めない場合、出力にはプレフィックス リストのエントリだけが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ルート マップとポリシー リストの一致基準としてルーティングでプレフィックス リストを使用します。

例

次に、**show prefix-list** コマンドの出力例を示します。

```
ciscoasa# show prefix-list
prefix-list prefix_1: 1 entries
   seq 1 permit 2.0.0.0/8
```

次に、要約された出力の例を示します。

```
ciscoasa# show prefix-list summary
Prefix-list with the last deletion/insertion: prefix_1
prefix-list prefix_1:   Description: FirstPrefixList
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3
```

次に、詳細な出力の例を示します。

```
ciscoasa# show prefix-list detail
Prefix-list with the last deletion/insertion: prefix_1
prefix-list prefix_1:   Description: FirstPrefixList
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3

   seq 1 permit 2.0.0.0/8 (hit count: 0, refcount: 1)
```

関連コマンド

コマンド	説明
prefix-list	プレフィックス リストを設定します。

show priority-queue

インターフェイスのプライオリティ キューの構成または統計情報を表示するには、特権 EXEC モードで **show priority-queue** コマンドを使用します。

show priority-queue {**config** | **statistics**} [*interface_name*]

構文の説明

config	インターフェイス プライオリティ キューのキューおよび TX-ring の制限を表示します。
interface_name	（オプション）構成、またはベストエフォート キューおよび低遅延キューの統計の詳細を表示するインターフェイスの名前を指定します。
statistics	ベストエフォート キューおよび低遅延キューの統計の詳細を表示します。

デフォルト

インターフェイス名を省略した場合は、すべての設定済みインターフェイスについての構成またはプライオリティ キュー統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、test という名前のインターフェイスの統計情報の例を示します。この出力で、BE はベストエフォート キュー、LLQ は低遅延キューを表しています。

```
ciscoasa# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
```

```
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
ciscoasa#
```

次に、設定されているすべてのインターフェイスのプライオリティ キューの構成を表示する例を示します。

```
ciscoasa# show priority-queue config

Priority-Queue Config interface inside
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface test
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface outside
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface bgmember1
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定されたインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
clear priority-queue statistics	プライオリティ キューの統計カウンタをクリアします。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

show processes

ASA 上で動作しているプロセスのリストを表示するには、特権 EXEC モードで **show processes** コマンドを使用します。

show processes [**cpu-usage** [[**non-zero**][**sorted**]] [**cpu-hog** | **memory** | **internals**]

構文の説明

cpu-hog	CPU を占有しているプロセス（CPU の使用時間が 100 ミリ秒を超えているプロセス）の番号および詳細を表示します。
cpu-usage	過去 5 秒間、1 分間、および 5 分間に各プロセスで使用された CPU のパーセンテージを表示します。
internals	各プロセスの内部詳細を表示します。
メモリ	各プロセスのメモリ割り当てを表示します。
non-zero	（任意）CPU 使用状況がゼロではないプロセスを表示します。
sorted	（オプション）プロセスの CPU 使用状況をソートして表示します。

デフォルト

デフォルトで、このコマンドは ASA で実行されているプロセスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.0(4)	ランタイム値が拡張され、1 ミリ秒以内の精度で表示されるようになりました。
7.2(1)	出力が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。
8.0(1)	**cpu-usage** キーワードが追加されました。
9.2(1)	出力が拡張され、CPU 占有検出情報が表示されるようになりました。

使用上のガイドライン

プロセスは、数個の命令だけを必要とする軽量スレッドです。次に示すように、**show processes** コマンドを使用すると、ASA 上で実行されているプロセスのリストが表示されます。

コマンド	表示されるデータ	説明
show processes	PC	プログラム カウンタ。
show processes	Stack Pointer	スタック ポインタ。
show processes	STATE	スレッド キューのアドレス。
show processes	Runtime	スレッドが CPU クロック サイクルに基づいて実行されている時間（ミリ秒）。クロック ティック（10 ミリ秒の精度）ではなく CPU クロック サイクル（10 ナノ秒未満の精度）に基づいてプロセスの CPU 使用状況を完全かつ正確に計算するため、精度は 1 ミリ秒以内です。
show processes	SBASE	スタック ベース アドレス。
show processes	Stack	現在使用中のバイト数とスタックの合計サイズ。
show processes	プロセス	スレッドの機能。
show processes cpu-usage	MAXHOG	最大 CPU 占有実行時間（ミリ秒）。
show processes cpu-usage	NUMHOG	CPU 占有実行数。
show processes cpu-usage	LASTHOG	最後の CPU 占有実行時間（ミリ秒）。
show processes cpu-usage	PC	CPU 占有プロセスの命令ポインタ。
show processes cpu-usage	Traceback	CPU 占有プロセスのスタック トレース。Traceback には最大で 14 のアドレスを設定できます。
show processes internals	Invoked Calls	スケジューラがプロセスを実行した回数。
show processes internals	Giveups	プロセスが CPU をスケジューラに返還した回数。

show processes cpu-usage コマンドを使用すると、ASA 上で ASA の CPU を使用している可能性のある特定のプロセスを絞り込むことができます。**sorted** コマンドおよび **non-zero** コマンドを使用すると、**show processes cpu-usage** コマンドの出力をさらにカスタマイズできます。

スケジューラと合計サマリー行で、**show proccesses** コマンドを 2 回連続で実行し、その出力を比較して次のことを判断できます。

- CPU の 100% の消費。
- スレッドのランタイム差分と合計ランタイム差分とを比較して決定された、各スレッドで使用されている CPU のパーセンテージ。

ASA は、多くの異なる実行スレッドを備えた単一のプロセスとして稼働します。このコマンドの出力は、実際に、スレッド単位でメモリ割り当てと空きメモリを示します。これらのスレッドは、データ フローおよび ASA の操作に関する他の操作において連携して動作するため、他のスレッドがメモリ ブロックを開放している間、別のスレッドがそのブロックを割り当てることができます。出力の最後の行には、すべてのスレッドの合計カウントが含まれます。割り当てと空きメモリとの差異を監視することで、メモリ リークの可能性を追跡するために、唯一この行を使用できます。

例

次に、ASA 上で実行されているプロセスのリストを表示する例を示します。

```
ciscoasa# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->

-     -        -         -        638515    -         -     scheduler
-     -        -         -       2625389    -         -     total
```

次に、各プロセスで使用されている CPU のパーセンテージを表示する例を示します。

```
ciscoasa# show proc cpu-usage non-zero
PC         Thread     5Sec    1Min    5Min    Process
0818af8e   d482f92c   0.1%    0.1%    0.1%    Dispatch Unit
08bae136   d48180f0   0.1%    0.0%    0.2%    ssh
-------------------------------------
```

次に、CPU を占有しているプロセスの数および詳細を表示する例を示します。

```
ciscoasa# show processes cpu-hog
Granular CPU hog detection currently running, started at 15:41:16 UTC Jan 6 2014.
    Sample count: 10000 Threshold: 10ms
Granular CPU hog detection completed at 15:41:16 UTC Jan 6 2014.
    Sample count: 10000 Threshold: 10ms
```

その他の CPU ホグ トレースバックは次のとおりです。

```
Process:      DATAPATH-0-2042, NUMHOG: 430, MAXHOG: 22, LASTHOG: 2
LASTHOG At:   15:42:21 UTC Jan 6 2014
PC:           0x0000000000000000 (suspend)
Call stack:   0x000000000041c98c  0x000000000041cc99  0x000000000069b0f0
              0x00000000013619af  0x0000000000136cbbd  0x0000000001372203
              0x00007ffffeab2f3a
              Interrupt based hog #1
              Hog #1, traceback #1, at:   15:41:16 UTC Jan 6 2014, hog 20 ms
              PC:           0x0000000000eb616b
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000ebcf71
                            0x0000000000ebc5ab  0x0000000000ebcb0e  0x0000000000e17410
                            0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
                            0x0000000001344419  0x000000000069b315  0x000000000069be9e
                            0x000000000069b0a4  0x00000000013619af
              Hog #1, traceback #2, at:   15:41:16 UTC Jan 6 2014, hog 21 ms
              PC:           0x0000000000e8fc41
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000e17410
                            0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
                            0x0000000001344419  0x000000000069b315  0x000000000069be9e
                            0x000000000069b0a4  0x00000000013619af  0x0000000000136cbbd
                            0x0000000001372203  0x00007ffffeab2f3a
              Interrupt based hog #2
              Hog #2, traceback #1, at:   15:41:36 UTC Jan 6 2014, hog 9 ms
```

```
PC:           0x0000000000eb6167
Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000ebcf71
              0x0000000000ebc5ab  0x0000000000ebcb0e  0x0000000000e17410
              0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
              0x0000000001344419  0x000000000069b315  0x000000000069be9e
              0x000000000069b0a4  0x00000000013619af
Interrupt based hog #3
Hog #3, traceback #1, at:   15:42:21 UTC Jan 6 2014, hog 2 ms
PC:           0x000000000068a223
Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x000000000069bbba
              0x000000000069b0a4  0x00000000013619af  0x000000000136cbbd
              0x0000000001372203  0x00007ffffeab2f3a
```

次に、各プロセスのメモリ割り当てを表示する例を示します。

```
ciscoasa# show processes memory

-------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
-------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
```

次に、各プロセスの内部詳細を表示する例を示します。

```
ciscoasa# show processes internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
```

```
        8973          8968  Checkheaps
           6             0  Session Manager
         237           235  uauth
(other lines deleted for brevity)
```

関連コマンド

コマンド	説明
show cpu	CPU 使用状況の情報を表示します。

show ptp

さまざまな PTP 統計情報とクロック関連情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show ptp** コマンドを使用します。

show ptp {**clock** | **internal-info** | **port** [*interface-name*]}

(注) このコマンドは、Cisco ISA 3000 アプライアンスにのみ適用されます。

構文の説明

clock	PTP クロックのプロパティを表示します。
internal-info	ポート固有のカウンタなど、PTP の内部情報を表示します。
port	PTP 対応のすべてのインターフェイスの PTP ポート情報を表示します。
interface-name	指定されたインターフェイスの PTP ポート情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

show ptp port コマンドにオプションのインターフェイス ID を含めると、そのインターフェイスのポート情報のみが表示されます。

また、グローバル コンフィギュレーション モードでは、**show ptp clock | port | internal-info** コマンドも使用できます。

例

次に、PTP クロック プロパティを表示する例を示します。

```
ciscoasa# show ptp clock
PTP CLOCK INFO
  PTP Device Type: Transparent Clock
  Operation mode: One Step
  Clock Identity: 0:8:2F:FF:FE:E8:43:81
  Clock Domain: 0
  Number of PTP ports: 4
```

次に、PTP 対応のすべてのインターフェイスの PTP ポート情報を表示する例を示します。

```
ciscoasa# show ptp port
PTP PORT DATASET: GigabitEthernet1/1
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 1
  PTP version: 2
  Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/2
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 2
  PTP version: 2
  Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/3
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 3
  PTP version: 2
  Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 4
  PTP version: 2
  Port state: Enabled
```

show quota management-session

現在の管理セッションの統計情報を表示するには、特権 EXEC モードで **how quota management-session** コマンドを使用します。

show quota management-session [**ssh** | **telnet** | **http** | **username** *user*]

構文の説明

ssh	SSH セッションを示します。
telnet	Telnet セッションを示します。
http	HTTP セッションを示します。
username *user*	特定のユーザのセッションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。
9.12(1)	このコマンドは、**quota management-session** コマンドがコンテキストごとにクォータをサポートするようになったため、コンテキスト内でのみ使用可能になりました。**ssh**、**telnet**、**http**、および **username** キーワードが追加されました。表示出力にはプロトコルごとのセッション数が表示されるようになりました。

使用上のガイドライン

このコマンドは、アクティブな管理セッションをタイプ別に表示します。

例

次に、現在の管理セッションの統計情報を表示する例を示します。

```
ciscoasa# show quota management-session
#Sessions               ConnectionType                  Username
1                             SSH                       cisco
2                             TELNET                    cisco
1                             SSH                       cisco1
```

関連コマンド

コマンド	説明
show running-config quota management-session	管理セッション クォータの現在の値を表示します。
quota management-session	デバイスで同時に実行できる ASDM、SSH、および Telnet セッションの数を設定します。

show raid

システムのハード ドライブの RAID ステータスに関する情報を表示するには、特権 EXEC モードで **show raid** コマンドを使用します。

show raid

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.1(1)	このコマンドが追加されました。

使用上のガイドライン

一部のハードウェア モデルは、2 つの内部ハード ドライブをサポートします。たとえば、ASA 5545-X および 5555-X は最大 2 つのソリッド ステート ドライブをサポートします。2 つのドライブが存在する場合、それらのドライブは RAID-1 設定で自動的にフォーマットされます。この構造は、デバイスをリロードするたびに再構築されます。RAID 設定に関する情報を表示するには、**show raid** コマンドを使用できます。

(注) デバイスのモデルが RAID をサポートしていない場合、**show raid** コマンドを入力すると無効なコマンドによるエラー メッセージが表示される場合があります。

次の表で、出力のフィールドについて説明します。

フィールド	説明
ID	アレイ コンポーネントの ID（例：/dev/md0）。
Version	Superblock（RAID メタ データ）のフォーマット。
Creation Time	このコンポーネントが設定された日時。
RAID レベル	RAID レベル。RAID1 はミラーリング構成です。

フィールド	説明
Array Size	すべてのコンポーネントのデバイスで使用可能な合計記憶域(バイト、ギビバイト、ギガバイト)。
Used Dev Size	各デバイスで合計容量に影響する記憶域の容量(バイト、ギビバイト、ギガバイト)。これは最小のデバイスまたはパーティションによって決まります。大きいデバイスには未使用のスペースがある場合があります。
RAID Devices	スペア、不足、障害が発生したデバイスを含む完全なアレイのメンバデバイスの合計数。
Total Devices	使用可能な機能デバイスの数。
Persistence	Superblock がアレイのすべてのコンポーネントのデバイスに特定の位置に書き込まれること持続性 Superblock(アレイが作成されたときのデフォルト)は、Superblock がアレイのすべてのコンポーネント デバイスで特定の位置に書き込まれることを意味します。その後、RAID 設定は関連ディスクから直接読み取ることができます。
Update Time	アレイのステータスが変更された時刻。ステータス変更には、アクティブ化、障害などが含まれます。
状態	RAID の現在のステータス。最初のステータスは、アレイが完全に動作している場合は **active**、アレイがアクティブでも保留中の書き込み操作がない場合は **clean** が示されます。 表示される可能性のあるステータスは次のとおりです。 • resyncing, active:システムが新しく、現在 RAID 構造を構築しています。必要な構造の構築に 90 分以上かかる場合があります。完了率を示す出力の Rebuild Status 行を探します。 • (clean または active), degraded, recovering:RAID 構造が正常に構築されました。 • (clean または active), degraded:1 つのハード ドライブが機能していません。壊れているか、または見つからないかのいずれかです。2 つのドライブを使用する場合は、壊れているか、または見つからないドライブを交換します。 • (clean または active), degraded, recovering:ハード ドライブの取り付けまたは交換後にシステムが RAID 構造を再構築しています。
Active Devices	アレイの現在の機能デバイスの数。予備のデバイスは含まれていません。
Working Devices	アレイの使用可能な(障害のない)デバイスの総数。つまり、アクティブ デバイスと予備のデバイス。
Failed Devices	アレイの障害の発生したデバイス。
Spare Devices	現在アレイに割り当てられている予備のデバイスの数。アレイのメンバーが見つからない場合は、使用可能なスペアをアクティブ メンバーとしてアレイ内に構築する必要があります。ただし、システムがアレイへのスペアの追加に失敗した場合、ドライブもスペアとしてマークされます。
UUID	128 ビットの 16 進数汎用一意識別子(UUID)はアレイの Superblock に格納されています。この番号は、ランダムに生成され、RAID を一意にタグ付けするために使用されます。すべてのコンポーネント デバイスがこの ID を共有します

フィールド	説明
Event	アレイのイベント カウンタ。Superblock が更新されるたびに増分されます。
Component table	コンポーネント ディスクの番号は 0 から始まります。メジャー番号は通常、デバイス タイプに対応し、マイナー番号は、そのグループ内の特定のデバイスの ID です。たとえば、「Major 8」は SCSI ディスクを示します。 RAID デバイスの各コンポーネントと、コンポーネントの現在のステータスのリストがここに表示されます。健全なディスクは、**active sync** 状態になっています。

例

次に、アクティブで稼働中のハード ドライブが 1 つある場合、State、Active Devices、および Working Devices の各行でどのように表示されるかの例を示します。また、最後のテーブルに示すように、2 番目のデバイスが「removed」の状態であることも出力に示されます。つまり、2 番目のドライブは取り付けられていなかったか、または 2 番目のドライブが実際に取り外されているかのいずれかです。

```
ciscoasa# show raid
/dev/md0:
        Version : 1.2
  Creation Time : Mon Mar  6 09:04:14 2017
     Raid Level : raid1
     Array Size : 124969216 (119.18 GiB 127.97 GB)
  Used Dev Size : 124969216 (119.18 GiB 127.97 GB)
   Raid Devices : 2
  Total Devices : 1
    Persistence : Superblock is persistent

  Intent Bitmap : Internal

    Update Time : Tue Mar 21 14:03:27 2017
          State : active, degraded
 Active Devices : 1
Working Devices : 1
 Failed Devices : 0
  Spare Devices : 0

           Name : ciscoasa:0  (local to host ciscoasa)
           UUID : e8f90a6b:20433f38:e8b86378:6fd52057
         Events : 454610

    Number   Major   Minor   RaidDevice State
       0       8        0        0      active sync   /dev/sda
       1       0        0        1      removed
```

show reload

ASA のリロードのステータスを表示するには、特権 EXEC モードで **show reload** コマンドを使用します。

show reload

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには使用上のガイドラインがありません。

例

次に、リロードが 4 月 20 日、土曜日の午前 0 時(夜の 12 時)にスケジューリングされている例を示します。

```
ciscoasa# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

関連コマンド

コマンド	説明
reload	コンフィギュレーションをリブートおよびリロードします。

show resource allocation

すべてのクラスとクラス メンバーにまたがってリソースごとにリソース割り当てを表示するには、特権 EXEC モードで **show resource allocation** コマンドを使用します。

show resource allocation [**detail**]

構文の説明

detail	追加情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.0(1)	新規リソース クラス routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。

使用上のガイドライン

このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際のリソース使用状況を表示するには、**show resource usage** コマンドを使用します。

例

次に、**show resource allocation** コマンドの出力例を示します。ディスプレイには、各リソースの合計割り当て値が、絶対値および使用可能なシステム リソースのパーセンテージとして表示されます。

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000         30.50%
 Hosts                      78842           N/A
 SSH                           35         35.00%
```

```
Telnet                          35           35.00%
Routes                       25000           0.00%
Xlates                       91749           N/A
Other VPN Sessions              20           2.66%
Other VPN Burst                 20           2.66%
All                      unlimited
```

表 11-2 に、各フィールドの説明を示します。

表 11-2　show resource allocation のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。クラス定義でパーセンテージを指定した場合、ASA はこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	使用できる場合は、すべてのコンテキストで割り当てられるシステム リソース総量のパーセンテージ。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

次に、**show resource allocation detail** コマンドの出力例を示します。

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A
```

```
SSH               default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                             20     20.00%

Telnet            default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                             20     20.00%
Routes            default          all       C  unlimited                N/A
                  gold               1       D  unlimited          5      N/A
                  silver             1      CA         10         10      N/A
                  bronze             0      CA          5                 N/A
                  All Contexts:      3                             20      N/A

Xlates            default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      23040      23040     N/A
                  bronze             0      CA      11520
                  All Contexts:      3                         23040     N/A

mac-addresses     default          all       C      65535
                  gold               1       D      65535      65535    100.00%
                  silver             1      CA       6553       6553      9.99%
                  bronze             0      CA       3276
                  All Contexts:      3                        137623    209.99%
```

表 11-3 に、各フィールドの説明を示します。

表 11-3　show resource allocation detail のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
クラス	デフォルト クラスを含む、各クラスの名前。 すべてのコンテキスト フィールドには、すべてのクラス全体での合計値が表示されます。
Mmbrs	各クラスに割り当てられるコンテキストの数。
Origin	リソース制限の生成元。値は次のとおりです。 • A:この制限を個々のリソースとしてではなく、**all** オプションを使用して設定します。 • C:この制限はメンバー クラスから生成されます。 • D:この制限はメンバー クラスでは定義されたのではなく、デフォルト クラスから生成されました。デフォルト クラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 ASA では、「A」と「C」または「D」を組み合わせることができます。
Limit	コンテキストごとのリソース制限(絶対数として)。クラス定義でパーセンテージを指定した場合、ASA はこの表示のためにパーセンテージを絶対数に変換します。

表 11-3　show resource allocation detail のフィールド(続き)

フィールド	説明
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。リソースが無制限の場合、この表示は空白です。
% of Avail	使用できる場合、クラス内のすべてのコンテキストにわたって割り当てられるシステム リソースの合計数のパーセンテージ。リソースが無制限の場合、この表示は空白です。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを追加します。
limit-resource	クラスのリソース制限を設定します。
show resource types	制限を設定できるリソース タイプを表示します。
show resource usage	ASA のリソース使用状況を表示します。

show resource types

ASA が使用状況の追跡対象にしているリソース タイプを表示するには、特権 EXEC モードで **show resource types** コマンドを使用します。

show resource types

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは、コンテキストごとに管理できる追加のリソース タイプを表示するように変更されました。
9.0(1)	新規リソース クラス routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。

例

次に、リソース タイプの例を示します。

```
ciscoasa# show resource types

Rate limited resource types:
  Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
```

```
Telnet          Telnet Sessions
Xlates          XLATE Objects
Routes          Routing Table Entries
Other-vpn       Other VPN licenses
Other-vpn-burst Allowable burst for Other VPN licenses
All             All Resources
```

関連コマンド

コマンド	説明
clear resource usage	リソース使用状況の統計情報をクリアします。
context	セキュリティ コンテキストを追加します。
show resource usage	ASA のリソース使用状況を表示します。

show resource usage

ASA またはマルチ モードの各コンテキストのリソース使用状況を表示するには、特権 EXEC モードで **show resource usage** コマンドを使用します。

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system** | **detail**] [**resource** {[**rate**] *resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

構文の説明

context *context_name*	(マルチ モードのみ)統計情報を表示するコンテキストの名前を指定します。すべてのコンテキストを対象にするには、**all** を指定します。ASA は、各コンテキストのリソース使用状況を一覧表示します。
count_threshold	表示するリソースの使用回数を設定します。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*count_threshold* は現在の使用状況に適用されます。 (注) すべてのリソースを表示するには、*count_threshold* を **0** に設定します。
counter *counter_name*	次のカウンタ タイプの数を表示します。 • **current**: リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。 • **peak**: ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後にクリアされた時点から計測されます。 • **denied**: Limit カラムに示されるリソース制限を超えたため拒否されたインスタンスの数を表示します。 • **all**: (デフォルト)すべての統計情報を表示します。
detail	管理できないリソースを含むすべてのリソースのリソース使用状況を表示します。たとえば、TCP 代行受信の数を表示できます。

resource [**rate**] *resource_name*	特定のリソースの使用状況を表示します。すべてのリソースを対象にするには、**all**（デフォルト）を指定します。リソースの使用状況を表示するには、**rate** を指定します。比率で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソース タイプを指定する場合は、**rate** キーワードを指定する必要があります。conns リソースは、同時接続としても測定されます。1 秒あたりの接続を表示するには、**rate** キーワードのみを使用します。 リソースには、次のタイプがあります。 • **asdm**：ASDM 管理セッション。 • **conns**：1 つのホストと複数のその他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • **inspects**：アプリケーション インスペクション。 • **hosts**：ASA を通じて接続可能なホスト。 • **mac-addresses**：トランスペアレント ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。 • **routes**：ルーティング テーブル エントリ。 • **ssh**：SSH セッション。 • **syslogs**：システム ログ メッセージ。 • **telnet**：Telnet セッション。 • （マルチ モードのみ）**VPN Other**：サイト間 VPN セッション。 • （マルチ モードのみ）**VPN Burst Other**：サイト間 VPN バースト セッション。 • **xlates**：NAT 変換。
summary	（マルチ モードのみ）すべてのコンテキストの合算使用状況を表示します。
システム	（マルチ モードのみ）すべてのコンテキストの合算使用状況を表示します。ただし、コンテキストの合算制限値ではなくシステムのリソース制限値を表示します。
top *n*	（マルチ モードのみ）指定したリソースの上位 *n* 人のユーザのコンテキストを表示します。このオプションでは、**resource all** ではなく、リソース タイプを 1 つのみ指定する必要があります。

デフォルト

マルチ コンテキスト モードでは、デフォルト コンテキストは **all** です。すべてのコンテキストのリソース使用状況が表示されます。シングル モードの場合、コンテキスト名は無視され、出力では「context」は「System」として表示されます。

デフォルトのリソース名は、**all** です。すべてのリソース タイプが表示されます。

デフォルトのカウンタ名は、**all** です。すべての統計情報が表示されます。

デフォルトのカウントしきい値は **1** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	コンテキストごとにリソースを制限できるため、このコマンドでは拒否されたリソースが表示されます。
9.0(1)	新規リソース クラス routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。

例

次に、**show resource usage context** コマンドの出力例を示します。ここでは、admin コンテキストのリソース使用状況を表示する例を示しています。

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

次に、**show resource usage summary** コマンドの出力例を示します。ここでは、すべてのコンテキストとすべてのリソースのリソース使用状況を表示する例を示しています。ここでは、6 コンテキスト分の制限値が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Inspects [rate]           270          535     100000(S)       0 Summary
Other VPN Sessions          0           10         10        740 Summary
Other VPN Burst             0           10         10        730 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage system** コマンドの出力例を示します。ここでは、すべてのコンテキストのリソース使用状況が表示されますが、合算のコンテキスト制限値ではなくシステム制限値が表示されています。

```
ciscoasa# show resource usage system

Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

次に、**show resource usage detail counter all 0** コマンドの出力例を示します。このコマンドは、ユーザが管理できるリソースだけでなく、すべてのリソースを表示します。

```
ciscoasa# show resource usage detail counter all 0

Resource              Current         Peak      Limit        Denied Context
memory                1012028      1538428  unlimited             0 admin
chunk:aaa                   0            0  unlimited             0 admin
chunk:aaa_queue             0            0  unlimited             0 admin
chunk:acct                  0            0  unlimited             0 admin
chunk:channels             25           39  unlimited             0 admin
chunk:CIFS                  0            0  unlimited             0 admin
chunk:conn                  0            0  unlimited             0 admin
chunk:crypto-conn           0            0  unlimited             0 admin
chunk:dbgtrace              1            2  unlimited             0 admin
chunk:dhcpd-radix           0            0  unlimited             0 admin
chunk:dhcp-relay-r          0            0  unlimited             0 admin
chunk:dhcp-lease-s          0            0  unlimited             0 admin
chunk:dnat                  0            0  unlimited             0 admin
chunk:ether                 0            0  unlimited             0 admin
chunk:est                   0            0  unlimited             0 admin

...

Telnet                      0            0          5             0 admin
SSH                         1            1          5             0 admin
ASDM                        0            1          5             0 admin
Syslogs [rate]              0           68  unlimited             0 admin
aaa rate                    0            0  unlimited             0 admin
url filter rate             0            0  unlimited             0 admin
Conns                       1            6  unlimited             0 admin
Xlates                      0            0  unlimited             0 admin
tcp conns                   0            0  unlimited             0 admin
Hosts                       2            3  unlimited             0 admin
Other VPN Sessions          0           10        750           740 admin
Other VPN Burst             0           10        750           730 admin
udp conns                   0            0  unlimited             0 admin
smtp-fixups                 0            0  unlimited             0 admin
Conns [rate]                0            7  unlimited             0 admin
establisheds                0            0  unlimited             0 admin
pps                         0            0  unlimited             0 admin
syslog rate                 0            0  unlimited             0 admin
bps                         0            0  unlimited             0 admin
Fixups [rate]               0            0  unlimited             0 admin
non tcp/udp conns           0            0  unlimited             0 admin
tcp-intercepts              0            0  unlimited             0 admin
globals                     0            0  unlimited             0 admin
np-statics                  0            0  unlimited             0 admin
statics                     0            0  unlimited             0 admin
nats                        0            0  unlimited             0 admin
ace-rules                   0            0        N/A             0 admin
aaa-user-aces               0            0        N/A             0 admin
```

```
filter-rules                0           0         N/A             0 admin
est-rules                   0           0         N/A             0 admin
aaa-rules                   0           0         N/A             0 admin
console-access-rul          0           0         N/A             0 admin
policy-nat-rules            0           0         N/A             0 admin
fixup-rules                 0           0         N/A             0 admin
aaa-uxlates                 0           0   unlimited             0 admin
CP-Traffic:IP               0           0   unlimited             0 admin
CP-Traffic:ARP              0           0   unlimited             0 admin
CP-Traffic:Fixup            0           0   unlimited             0 admin
CP-Traffic:NPCP             0           0   unlimited             0 admin
CP-Traffic:Unknown          0           0   unlimited             0 admin
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
clear resource usage	リソース使用状況の統計情報をクリアします。
context	セキュリティ コンテキストを追加します。
limit-resource	クラスのリソース制限を設定します。
show resource types	リソース タイプのリストを表示します。

show rest-api agent

REST API エージェントが現在イネーブルになっているかどうかを判断するには、特権 EXEC モードで **show rest-api agent** コマンドを使用します。

show rest-api agent

(注) このコマンドは、ASAv のすべてのバージョン、ASA 5585-X、および ASA 5500-X シリーズ（ASA 5506-X と ASA 5508-X を除く）のデバイスでサポートされます。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	対応	—	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、REST API エージェントが現在イネーブルになっているかどうかを判断するために使用します。

例

この例は、REST API エージェントがイネーブルになっていることを示しています。

```
ciscoasa(config)# show rest-api agent
REST API agent is currently enabled.
```

エージェントがディセーブルになっている場合に表示されるメッセージは、「REST API agent is currently disabled.」です。

関連コマンド

コマンド	説明
rest-api	REST API パッケージを確認してインストールします。REST API エージェントをイネーブルにします。
show version	REST API エージェントがイネーブルになっている場合、そのバージョン番号が **show version** 出力に含まれます。

show rip database

RIP トポロジ データベースに格納されている情報を表示するには、特権 EXEC モードで **show rip database** コマンドを使用します。

show rip database [*ip_addr* [*mask*]]

構文の説明

ip_addr	(任意)指定したネットワーク アドレスの表示ルートを制限します。
mask	(任意)オプションのネットワーク アドレスのネットワーク マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

RIP ルーティング関連の **show** コマンドは、ASA 上で特権 EXEC モードで使用できます。RIP 関連の **show** コマンドを使用する場合に RIP コンフィギュレーション モードである必要はありません。

RIP データベースには RIP を通じて学習されたルートがすべて含まれます。このデータベースに表示されるルートはルーティング テーブルには必ずしも表示されません。ルーティング テーブルにルーティング プロトコル データベースから値を挿入する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次に、**show rip database** コマンドの出力例を示します。

```
ciscoasa# show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
```

```
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

次に、ネットワーク アドレスとマスクを指定した、**show rip database** コマンドの出力例を示します。

```
Router# show rip database 172.19.86.0 255.255.255.0

172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

関連コマンド

コマンド	説明
router rip	RIP ルーティングをイネーブルにし、グローバル RIP ルーティング パラメータを設定します。

show rollback-status

Cisco Security Manager がロールバック要求を ASA に送信すると、Cisco Security Manager から ASA への管理接続がリセットされます。ロールバック ジョブの結果を Cisco Security Manager に送信することはできません。**show rollback-status** を使用して、ASA を照会するときに Cisco Security Manager にロールバック ジョブのステータスを表示します。

show rollback-status [*context_name*]

構文の説明

context_name	ロールバック ジョブが適用されるコンテキストの名前。シングル モードの場合、これは適用されません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	Admin/User Context	システム
設定	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.6(3)	このコマンドが導入されました。

使用上のガイドライン

show rollback-status を使用して、ロールバック ジョブのステータス、開始時刻、終了時刻、およびロールバック ジョブが適用されているコンテキスト名を表示します。

例

次に、シングル モードで入力されたすべてのコンテキストのロールバック ステータスを表示する例を示します。

1. Cisco Security Manager からのロールバック要求が受信される前は、次の状態です。

```
ciscoasa(config)# sh rollback-status
Status      : None
Start Time  : N/A
End Time    : N/A
```

2. ASA で最初のロールバック要求を受信すると、ジョブが完了する前は、次の状態です。

```
ciscoasa(config)# sh rollback-status
Status      : In Progress
Start Time  : 13:00:12 UTC May 11 2017
End Time    : N/A
```

3. ロールバック ジョブが完了したときは、次の状態です。

```
ciscoasa(config)# sh rollback-status
Status      : Succeeded
Start Time  : 13:00:12 UTC May 11 2017
End Time    : 13:00:14 UTC May 11 2017
```

4. ロールバックが失敗した場合、出力は次のようになります。

```
ciscoasa(cfg-cluster)# sh rollback-status
Status      : Failed
Start Time  : 13:25:49 UTC May 11 2017
End Time    : 13:25:55 UTC May 11 2017
```

5. ロールバックが失敗し、スタートアップ コンフィギュレーションに戻ると、次の状態です。

```
ciscoasa(cfg-cluster)# sh rollback-status
Status      : Reverted ( Roll back failed, startup config applied )
Start Time  : 13:25:49 UTC May 11 2017
End Time    : 13:25:55 UTC May 11 2017
```

次の例は、マルチモードで system/admin コンテキストから入力されたロールバック ステータスを示しています。

1. ロールバックを ASA に展開する前は、次の状態です。

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : None
Start Time  : N/A
End Time    : N/A

Context Name: admin
Status      : None
Start Time  : N/A
End Time    : N/A

Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A

Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

2. システム コンテキストのロールバックが開始された時点では、次の状態です。

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : In Progress
Start Time  : 16:55:35 UTC May 11 2017
End Time    : N/A

Context Name: admin
Status      : None
Start Time  : N/A
End Time    : N/A

Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
```

```
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

3. システム コンテキストのロールバックが完了した時点では、次の状態です。

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : Succeeded
Start Time  : 19:52:25 UTC May 11 2017
End Time    : 19:52:34 UTC May 11 2017

Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017

Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A

Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

4. コマンドでコンテキスト名が指定されている場合は、次の状態です。

```
ciscoasa(config)# sh rollback-status system
Context Name: system
Status      : Succeeded
Start Time  : 19:52:25 UTC May 11 2017
End Time    : 19:52:34 UTC May 11 2017

ciscoasa(config)# sh rollback-status admin
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

次の例は、マルチモードで admin/user コンテキストから入力されたロールバック ステータスを示しています。

1. コンテキスト名が指定されていない場合は、次の状態です。

```
ciscoasa/admin(config)# sh rollback-status
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

2. コンテキスト名が指定されている場合は、次の状態です。

```
ciscoasa/admin(config)# sh rollback-status admin
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

3. 誤ったコンテキスト名が指定されている場合は、次の状態です。

```
ciscoasa/admin(config)# sh rollback-status ad
Context ad does not exist.
```

4. コンテキスト名が現在のコンテキストと一致しない場合は、次のようになります。

```
ciscoasa/admin(config)# sh rollback-status ctx1
Context ctx1 does not match current context.
```

ASA がスレーブまたはスタンバイ装置として動作している場合は、警告メッセージが表示されます。

1. スレーブから show コマンドが発行されると、出力は次のようになります。

```
ciscoasa(config)# sh rollback-status
WARNING: Current unit is Slave.
```

2. スタンバイから show コマンドが発行されると、出力は次のようになります。

```
ciscoasa(config)# sh rollback-status
WARNING: Current unit is Standby.
```

次の表で出力エントリの詳細について説明します。

出力	説明
Context Name	ロールバック ジョブが適用されるコンテキストの名前。シングル モードの場合、これは表示されません。
Status（ステータス）	最新のロールバック ジョブのステータス。次のいずれかになります。 • [None]：このコンテキストにロールバック ジョブは導入されていません。 • [In Progress]：ASA が Cisco Security Manager からロールバック要求を受信し、ロールバック ジョブが進行中です。 • [Succeeded]：ロールバックが正常に完了しました。 • [revert]：Cisco Security Manager から送信された設定へのロールバックが失敗し、ASA に保存されいるスタートアップ設定へのロールバックがトリガーされ、この復元アクションが正常に完了し、ASA は現在スタートアップ設定で実行されています。 • [Failed]：ロールバックはエラーが発生して完了しました。
Start Time	直近のロールバック ジョブの開始時刻。ASA でロールバック ジョブを受信するたびに、このフィールドは ASA の現在の時刻で更新されます。ステータスは [In Progress] として更新されます。ロールバックが None 状態の場合、[N/A] が表示されます。
End Time	ロールバック ジョブが完了した時刻。ジョブがエラーなしで完了した場合、[Status] は [Succeeded] として更新されます。ロールバック中に復元アクションが実行され、復元が正常に完了した場合、ステータスは [Reverted] として更新されます。復元に失敗した場合、ステータスは [Failed] として更新されます。[None] または [In Progress] 状態のロールバックの場合は、[N/A] が表示されます。

show route

ルーティング テーブルを表示するには、特権 EXEC モードで **show route** コマンドを使用します。

show route [**management-only** [*interface_name*]] [**cluster** | **failover** | *ip_address* [*mask*] [**longer-prefixes**] | **bgp** [*as_number*] | **connected** | **eigrp** [*process_id*] | **isis** | **isis** | **ospf** [*process_id*] | **rip** | **static** | **summary** | **zone**]

構文の説明

bgp *as_number*	(オプション)ルーティング情報ベース(RIB)エポック番号(シーケンス番号)、現在のタイマー値、および BGP ルートのネットワーク記述子ブロック エポック番号(シーケンス番号)を表示します。*as_number* は、表示対象を指定の AS 番号を使用するルート エントリに限定します。
クラスタ	(オプション)ルーティング情報ベース(RIB)エポック番号(シーケンス番号)、現在のタイマー値、およびネットワーク記述子ブロック エポック番号(シーケンス番号)を表示します。
接続	(任意)接続されているルートを表示します。
eigrp *process_id*	(オプション)EIGRP ルートを表示します。
フェールオーバー	(オプション)フェールオーバーが発生してスタンバイ ユニットがアクティブ ユニットになった場合の、ルーティング テーブルおよびルーティング エントリの現在のシーケンス番号を表示します。
interface_name	(オプション)指定したインターフェイスを使用するルート エントリを表示します。
ip_address mask	(オプション)指定された宛先へのルートを表示します。
isis	(オプション)IS-IS ルートを表示します。
longer-prefixes	(オプション)指定された *ip_address*/*mask* ペアに一致するルートのみを表示します。
management-only	(オプション)IPv4 管理ルーティング テーブル内のルートを表示します。
isis	(オプション)IS-IS ルートを表示します。
ospf *process_id*	(オプション)OSPF ルートを表示します。
rip	(オプション)RIP ルートを表示します。
静的	(任意)スタティック ルートを表示します。
summary	(任意)ルーティング テーブルの現在の状態を表示します。
zone	(オプション)ゾーン インターフェイスのルートを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	**eigrp** キーワードが追加されました。
8.4(1)	**failover** キーワードが追加されました。出力には、RIB エポック番号（シーケンス番号）、現在のタイマー値、ネットワーク記述子ブロック エポック番号（シーケンス番号）が表示されます。
9.0(1)	**cluster** キーワードが追加されました。ダイナミック ルーティング プロトコル（EIGRP、OSPF、および RIP）に適用され、ASA 5580 および 5585-X でのみ使用できます。
9.2(1)	キーワード **bgp** が追加されました。
9.2(1)	このコマンドでは、ローカル ホスト ルートが、**接続された**ルートとともに表示されるようになりました。表示されるルートのプロトコルまたはタイプを示す新しいコード（L、I、E、su、および +）が追加されました。
9.3(2)	**zone** キーワードが追加されました。
9.5(1)	管理ルーティング テーブル機能のサポートが追加されました。
9.6(1)	**isis** キーワードが追加されました。
9.6(1)	**isis** キーワードが追加されました。

使用上のガイドライン

IPv4 に固有の情報である点を除いて、**show ipv6 route** コマンドの出力は、**show route** コマンドの出力と類似しています。

（注） ASA で対応する機能が設定されていない場合、**clustering** および **failover** キーワードは表示されません。

show route コマンドは、新しい接続の最適なルートを表示します。許可される TCP SYN をバックアップ インターフェイスに送信すると、ASA は同じインターフェイスを使用してのみ応答できます。そのインターフェイスの RIB にデフォルト ルートがない場合、ASA は隣接情報がないためにパケットをドロップします。**show running-config route** コマンドで表示されるよう設定されたものはすべて、システム内で特定のデータ構造で管理されます。

show asp table routing コマンドを使用して、バックエンド インターフェイスに固有のルーティング テーブルを確認できます。この設計は OSPF や EIGRP と同様であり、プロトコル固有のルート データベースは、「最適」ルートだけを表示するグローバル ルーティング テーブルとは異なります。この動作は設計によるものです。

(注) Cisco IOS で **show ip route** コマンドを使用する場合、**longer-prefix** キーワードを使用できます。Cisco IOS でこのキーワードを使用すると、ルートは、指定したネットワークとマスクのペアが一致したときにのみ表示されます。

ASA では、**longer-prefix** キーワードは **show route** コマンドのデフォルトの動作です。したがって、CLI でキーワードを追加する必要はありません。このため、**ip** を入力するとルートは表示されません。スーパーネット ルートを取得するには、マスク値を IP アドレスとともに渡す必要があります。

例

次に、**show route** コマンドの出力例を示します。

```
ciscoasa# show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

次に、管理コンテキストにおける ASA 5555 での **show route** コマンドの出力例を示します。この出力には、個々のユーザ認証用に VPN ハードウェア クライアントで使用される内部ループバック アドレスが表示されます。

```
ciscoasa/admin(config)# show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

次に、**show route bgp** コマンドの出力例を示します。

```
ciscoasa# show route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.116.1 to network 0.0.0.0
```

次に、**show route** の **failover** コマンドの出力例を示します。これは、フェールオーバー後のスタンバイ ユニットへの OSPF および EIGRP ルートの同期を示しています。

```
ciscoasa(config)# show route failover

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)

S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                        [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 1

O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0

D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

次に、**show route cluster** コマンドの出力例を示します。

```
ciscoasa(cfg-cluster)# show route cluster

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route


Gateway of last resort is not set

Routing table seq num 2
Reconvergence timer expires in 52 secs

C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

次に、**show route summary** コマンドの出力例を示します。

```
ciscoasa# show route summary

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

show route zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

次に、**show route isis** コマンドの出力例を示します。

```
ciscoasa# show route isis


Routing Table:
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is not set

i L2     1.1.1.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     2.2.2.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     3.3.3.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     4.4.4.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     5.5.5.0 255.255.255.0 [115/10] via 22.22.22.5, subint
```

show running-config コマンドから show sw-reset-button コマンドまで

show running-config

ASA 上で現在実行されているコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config** コマンドを使用します。

show running-config [**all**] [*command*]

構文の説明

all	デフォルトを含め、動作設定全体を表示します。
command	特定のコマンドに関連付けられたコンフィギュレーションを表示します。使用可能なコマンドについては、**show running-config ?** を使用して CLI ヘルプを参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.3(1)	暗号化されたパスワードが出力に追加されました。

リリース	変更内容
9.7(1)	このコマンドの出力も、IPv6 アドレスで設定された syslog サーバを表示します。
9.13(1)	• テレメトリ設定の詳細が出力に含まれています。 • 新しいコマンド:設定されたブロックサイズ値(デフォルト値を除く)を表示する **tftp blocksize** が追加されました。

使用上のガイドライン

show running-config コマンドは、ASA のメモリにあるアクティブなコンフィギュレーション(保存されたコンフィギュレーションの変更を含む)を表示します。

ASA のフラッシュ メモリに保存されたコンフィギュレーションを表示するには、**show configuration** コマンドを使用します。

show running-config コマンドの出力では、パスワードの暗号化がイネーブルかディセーブルかに応じて、パスワードが暗号化、マスク、またはクリア テキストの状態で表示されます。

(注) このコマンドを使用して ASA への接続または設定を行った後は、コンフィギュレーションに ASDM コマンドが表示されます。

ASA リリース 9.3 でディセーブルに変更された **error-recovery disable** のデフォルトです。そのため、WebVPN error recovery がデフォルト値の場合、**show running-config** コマンドは *error-recovery disable* を CLI に 表示するようになりました。問題のトラブルシューティング時にシスコのテクニカル アシスタンス センターからの指示がない限り、これはディセーブルのままにしておくことを推奨します。

ASA 9.13(1) 以降、このコマンドの出力にはテレメトリの詳細が含まれていました。**show running-config** コマンドには、テレメトリサービスのデフォルト以外の設定(**no service telemetry**)のみが表示されます。**all** コマンドを使用すると、デフォルトのテレメトリサービス設定も一緒に表示されます。

例

次に、**show running-config** コマンドの出力例を示します。

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.0(1)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.1.1.2 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.3 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
```

```
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname example1
domain-name example.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.1.1.2
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map abc_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
```

```
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy abc_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

次に、**show running-config access-group** コマンドの出力例を示します。

```
ciscoasa# show running-config access-group
access-group 100 in interface outside
```

次に、**show running-config arp** コマンドの出力例を示します。

```
ciscoasa# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
show configuration	スタートアップ コンフィギュレーションを表示します。

show saml metadata

SAML メタデータのトンネル グループ名を表示します。

show saml metadata tunnel-group-name

構文の説明

SAML メタデータを表示するトンネル グループの名前を入力します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

特定のトンネル グループの SAML SP のメタデータを表示します。

例

show scansafe server コマンドのサンプル出力を次に示します。

```
ciscoasa# show saml metadata saml_sso_tunnel_group
```

関連コマンド

コマンド	説明
saml idp	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。

show scansafe server

クラウド Web セキュリティ プロキシ サーバのステータスを表示するには、特権 EXEC モードで **show scansafe server** コマンドを使用します。

show scansafe server

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。

マルチ コンテキスト モードでは、このコマンドの出力は、ScanSafe サーバに到達する管理コンテキストの機能によって異なります。管理コンテキストは、定期的にポーリングを試行して、トラフィックが ASA を通過していない場合に ScanSafe サーバがアップしているかどうかを確認します。ポーリング試行の間隔は設定不可で、15 分に固定されています。また、管理コンテキストは、ScanSafe タワーにキープアライブを送信します。

例

show scansafe server コマンドのサンプル出力を次に示します。

```
ciscoasa# show scansafe server
ciscoasa# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
ciscoasa# Backup: proxy137.scansafe.net (80.254.152.99)
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

show scansafe statistics

クラウド Web セキュリティ アクティビティに関する情報を表示するには、特権 EXEC モードで **show scansafe statistics** コマンドを使用します。

show scansafe statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show scansafe statistics コマンドは、プロキシ サーバにリダイレクトされる接続数、現在リダイレクトされている接続数、ホワイトリストに記載されている接続数などのクラウド Web セキュリティ アクティビティに関する情報を示します。

例

次に、**show scansafe statistics** コマンドの出力例を示します。

```
ciscoasa# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

show sctp

現在の Stream Control Transmission Protocol（SCTP）Cookie とアソシエーションを表示するには、特権 EXEC モードで **show sctp** コマンドを使用します。

show sctp [**detail**]

構文の説明

detail	SCTP アソシエーションに関する詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。
9.7(1)	詳細な出力に、マルチホーミング、複数のストリーム、およびフレームリアセンブルに関する情報が含まれるようになりました。

使用上のガイドライン

show sctp コマンドは、SCTP Cookie とアソシエーションに関する情報を表示します。

例

次に、**show sctp** コマンドの出力例を示します。

```
ciscoasa# show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)

AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

次に、**show sctp detail** コマンドの出力例を示します。

```
ciscoasa(config)# show sctp detail

AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
    Cumulative TSN: 5cb6cd98
    Next TSN: 0
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
```

9.7(1) から、詳細な出力に、マルチホーミング、複数のストリームおよびフレーム リアセンブルに関する情報が含まれるようになりました。

```
asa2005# show sctp detail

AssocID: 2e590263
Local:  10.0.103.250/50000 (ESTABLISHED)
    Multi-homing IP's: 10.0.103.251(10.0.103.251)
    Receiver Window: 106496
    Cumulative TSN: bf0a3180
    Next TSN: 0
    Earliest Outstanding TSN: 0
    Re-ordering queue:
    Stream ID 3: next SN 10, first/last queued SN 11/16, hole SN:
    Stream ID 4: next SN 10, first/last queued SN 11/16, hole SN:
Remote: 10.0.102.250/3868 (CLOSED)
    Multi-homing IP's: 10.0.102.251(10.0.102.251)
    Receiver Window: 106496
    Cumulative TSN: 915d5916
    Next TSN: 0
    Earliest Outstanding TSN: 0
    Re-ordering queue:
Secondary Conn List:
    10.0.102.251(10.0.102.251):3868 to 10.0.103.251(10.0.103.251):50000
    10.0.103.251(10.0.103.251):50000 to 10.0.102.251(10.0.102.251):3868
    10.0.102.250(10.0.102.250):3868 to 10.0.103.251(10.0.103.251):50000
    10.0.103.251(10.0.103.251):50000 to 10.0.102.250(10.0.102.250):3868
    10.0.102.251(10.0.102.251):3868 to 10.0.103.250(10.0.103.250):50000
    10.0.103.250(10.0.103.250):50000 to 10.0.102.251(10.0.102.251):3868
```

関連コマンド

コマンド	説明
show local-host	インターフェイスごとに、ASA 経由で接続を確立しているホストの情報を表示します。
show service-policy inspect sctp	SCTP インスペクションの統計情報を表示します。
show traffic	インターフェイスごとに、接続とインスペクションの統計情報を表示します。

show service-policy

サービス ポリシー統計情報を表示するには、特権 EXEC モードで **show service-policy** コマンドを使用します。

show service-policy [**global** | **interface** *intf*] [**csc** | **cxsc** | **inspect** *inspection* [*arguments*] | **ips** | **police** | **priority** | **set connection** [**details**] | **sfr** | **shape** | **user-statistics**]

show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

構文の説明

csc	(オプション)**csc** コマンドを含むポリシーに関する詳細情報を表示します。
cxsc	(オプション)**cxsc** コマンドを含むポリシーに関する詳細情報を表示します。
dest_ip dest_mask	**flow** キーワードに対する宛先 IP アドレスおよびトラフィック フローのネットマスク。
details	(オプション)**set connection** キーワードの場合、クライアントごとの接続制限がイネーブルな場合に、クライアントごとの接続情報を表示します。
eq *dest_port*	**flow** キーワードの場合、この値に等しいフローの宛先ポートに相当します。
eq *src_port*	(オプション)**flow** キーワードの場合、この値に等しいフローの送信元ポートに相当します。
flow *protocol*	(オプション)5 つのタプル(プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート)で識別される特定フローに一致するポリシーを示します。このコマンドを利用すると、サービス ポリシー コンフィギュレーションによって、必要なサービスが特定の接続に提供されることを確認できます。 フローが 5 つのタプルとして示されるため、すべてのポリシーがサポートされるわけではません。次のサポート対象ポリシーが一致します。 • **match access-list** • **match port** • **match rtp** • **match default-inspection-traffic**
global	(オプション)出力をグローバル ポリシーに制限します。
host *dest_host*	**flow** キーワードに対するトラフィック フローのホスト宛先 IP アドレス。
host *src_host*	**flow** キーワードに対するトラフィック フローのホスト送信元 IP アドレス。
icmp_control_message	(オプション)プロトコルとして ICMP を指定した場合の **flow** キーワードに対して、トラフィック フローの ICMP 制御メッセージを指定します。
icmp_number	(オプション)プロトコルとして ICMP を指定した場合の **flow** キーワードに対して、トラフィック フローの ICMP プロトコル番号を指定します。

inspect *inspection* [*arguments*]	(オプション)**inspect** コマンドを含むポリシーに関する詳細情報を表示します。詳細出力では、一部の **inspect** コマンドはサポートされません。すべてのインスペクションを表示するには、引数を使用せずに **show service-policy** コマンドを使用します。各インスペクションで使用できる引数は異なります。詳細については、CLI ヘルプを参照してください。
interface *intf*	(任意)*intf* 引数で指定したインターフェイスに適用されるポリシーを表示します。*intf* は **nameif** コマンドで定義したインターフェイス名です。
ips	(オプション)**ips** コマンドを含むポリシーに関する詳細情報を表示します。
police	(オプション)**police** コマンドを含むポリシーに関する詳細情報を表示します。
priority	(オプション)**priority** コマンドを含むポリシーに関する詳細情報を表示します。
set connection	(オプション)**set connection** コマンドを含むポリシーに関する詳細情報を表示します。
sfr	(オプション)**sfr** コマンドを含むポリシーに関する詳細情報を表示します。
shape	(オプション)**shape** コマンドを含むポリシーに関する詳細情報を表示します。
src_ip src_mask	**flow** キーワードに対する送信元 IP アドレスおよびトラフィック フローで使用されるネットマスク。
user-statistics	(オプション)**user-statistics** コマンドを含むポリシーに関する詳細情報を表示します。このコマンドは、アイデンティティ ファイアウォールに関するユーザ統計情報を表示します。これには、選択したユーザの、送信パケット数、送信ドロップ数、受信パケット数および送信ドロップ数が含まれます。

デフォルト

引数を指定しない場合、このコマンドはすべてのグローバル ポリシーおよびインターフェイス ポリシーを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	**csc** キーワードが追加されました。

リリース	変更内容
7.2(4)/8.0(4)	**shape** キーワードが追加されました。
8.4(2)	アイデンティティ ファイアウォール用の **user-statistics** キーワードのサポートが追加されました。
8.4(4.1)	ASA CX モジュール用の **cxsc** キーワードのサポートが追加されました。
9.2(1)	ASA FirePOWER モジュール用の **sfr** キーワードのサポートが追加されました。
9.5(2)	**inspect sctp** および **inspect diameter** キーワードが追加されました。
9.6(2)	**inspect stun** および **inspect m3ua** {**drops** | **endpoint** *ip_address*} キーワードが追加されました。
9.7(1)	**inspect m3ua session** キーワードと **inspect gtp pdpmcb teid** *teid* キーワードが追加されました。また、表示ルールの制限がクラス マップあたり 64 から 128 に引き上げられました。
9.10(1)	dns を検査する **detail** キーワードが追加されました。Cisco Umbrella に関する詳細が提供されます。

使用上のガイドライン

show service-policy コマンドの出力に表示される初期接続の数は、**class-map** コマンドによって定義されたトラフィック マッチングに一致するインターフェイスへの、初期接続の数を示しています。「embryonic-conn-max」フィールドには、モジュラ ポリシー フレームワークを使用するトラフィック クラスに設定された最大初期接続の制限値が表示されます。表示される現在の初期接続数が最大値と等しい場合、または最大値を超えている場合は、新しい TCP 接続が **class-map** コマンドによって定義されたトラフィック タイプに一致すると、その接続に対して TCP 代行受信が適用されます。

コンフィギュレーションに対してサービス ポリシーの変更を加えた場合は、すべての*新しい*接続で新しいサービス ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。**show** コマンドの出力には、古い接続に関するデータが含まれていません。たとえば、インターフェイスから QoS サービス ポリシーを削除し、変更したバージョンを再度追加した場合、**show service-policy** コマンドには、新しいサービス ポリシーに一致する新しい接続に関連付けられた QoS カウンタだけが表示されます。古いポリシーの既存の接続はコマンド出力には表示されなくなります。すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** または **clear local-host** コマンドを参照してください。

(注) **inspect icmp** および **inspect icmp error** ポリシーの場合、パケット数にはエコー要求パケットと応答パケットのみが含まれます。

例

次に、**show service-policy global** コマンドの出力例を示します。

```
ciscoasa# show service-policy global

Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
```

次に、**show service-policy priority** コマンドの出力例を示します。

```
ciscoasa# show service-policy priority

Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap
```

次に、**show service-policy flow** コマンドの出力例を示します。

```
ciscoasa# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

次に、**show service-policy inspect http** コマンドの出力例を示します。この例では、match-any クラス マップ内の match コマンドごとに統計情報が表示されます。

```
ciscoasa# show service-policy inspect http

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http http, packet 1916, drop 0, reset-drop 0
        protocol violations
          packet 0
        class http_any (match-any)
          Match: request method get, 638 packets
          Match: request method put, 10 packets
          Match: request method post, 0 packets
          Match: request method connect, 0 packets
          log, packet 648
```

複数の CPU コアを搭載しているデバイスの場合は、ロック失敗用のカウンタがあります。共有されるデータ構造と変数は複数のコアによって使用可能なため、それらを保護するためにロック メカニズムが使用されます。コアはロックの取得に失敗すると、ロックの取得を再試行します。ロック失敗カウンタは、試行が失敗するごとに増分されます。

```
ciscoasa# show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

次に、**show service-policy inspect waas** コマンドの出力例を示します。この例では、waas の統計情報が表示されます。

```
ciscoasa# show service-policy inspect waas

Global policy:
  Service-policy: global_policy
    Class-map: WAAS
      Inspect: waas, packet 12, drop 0, reset-drop 0
        SYN with WAAS option 4
        SYN-ACK with WAAS option 4
        Confirmed WAAS connections 4
        Invalid ACKs seen on WAAS connections 0
        Data exceeding window size on WAAS connections 0
```

次に、GTP インスペクションの統計情報を表示するコマンドを示します。出力については、表 12-1 で説明されています。

```
firewall(config)# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

表 12-1　GPRS GTP 統計情報

カラムのヘッダー	説明
version_not_support	サポートされていない GTP バージョン フィールドを持つパケットの数を表示します。
msg_too_short	長さが 8 バイトより短いパケットの数を表示します。
unknown_msg	不明なタイプのメッセージ数を表示します。

表 12-1　GPRS GTP 統計情報（続き）

カラムのヘッダー	説明
unexpected_sig_msg	予期しないシグナリング メッセージ数を表示します。
unexpected_data_msg	予期しないデータ メッセージ数を表示します。
mandatory_ie_missing	必須情報要素（IE）が欠落しているメッセージ数を表示します。
mandatory_ie_incorrect	不正な形式の必須情報要素（IE）を持つメッセージ数を表示します。
optional_ie_incorrect	無効なオプション情報要素（IE）を持つメッセージ数を表示します。
ie_unknown	不明な情報要素（IE）を持つメッセージ数を表示します。
ie_out_of_order	順番どおりでない情報要素（IE）を持つメッセージ数を表示します。
ie_unexpected	予期しない情報要素（IE）を持つメッセージを表示します。
ie_duplicated	重複した情報要素（IE）を持つメッセージ数を表示します。
optional_ie_incorrect	不正な形式のオプション情報要素（IE）を持つメッセージ数を表示します。
total_dropped	ドロップされたメッセージの合計数を表示します。
signalling_msg_dropped	ドロップされた信号メッセージ数を表示します。
data_msg_dropped	ドロップされたデータ メッセージ数を表示します。
total_forwarded	転送されたメッセージの合計数を表示します。
signalling_msg_forwarded	転送された信号メッセージ数を表示します。
data_msg_forwarded	転送されたデータ メッセージ数を表示します。
total created_pdp	作成されたパケット データ プロトコル（PDP）またはベアラー コンテキストの合計数を表示します。
total deleted_pdp	削除されたパケット データ プロトコル（PDP）またはベアラー コンテキストの合計数を表示します。

表 12-1　GPRS GTP 統計情報（続き）

カラムのヘッダー	説明
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	これらのフィールドは、実装機能である PDP マスター制御ブロックの使用に関連しています。これらのカウンタは、トラブルシューティング向けにシスコ テクニカル サポートによって使用され、エンドユーザには直接の関係はありません。
pdp_non_existent	存在しない PDP コンテキストに対して受信したメッセージ数を表示します。

次に、PDP コンテキストに関する情報を表示するコマンドを示します。

```
ciscoasa# show service-policy inspect gtp pdp-context
1 in use, 32 most used

Version TID                 MS Addr         SGSN Addr    Idle     Timeout   APN
v2      2692026893437055 10.0.0.1        10.0.0.11       0:00:11  0:04:00
gprs.example.com
```

ASA 9.6.2 以降、GTP PDP コンテキスト情報はテーブルではなく、1 行ずつ示されます。このため、IPv6 アドレスの使用時に、情報が読み取り易くなります。

```
ciscoasa# show service-policy inspect gtp pdp-context
4 in use, 5 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

表 12-2 に、**show service-policy inspect gtp pdp-context** コマンドの出力の説明を示します。

表 12-2　PDP コンテキスト

カラムのヘッダー	説明
バージョン	GTP のバージョンを表示します。
TID	トンネル識別子を表示します。
MS Addr	モバイル ステーションのアドレスを表示します。
SGSN Addr SGW Addr	サービング ゲートウェイ サービス ノード（SGSN）またはサービング ゲートウェイ（SGW）を表示します。

表 12-2　PDP コンテキスト(続き)

カラムのヘッダー	説明
Idle	PDP またはベアラー コンテキストが使用されていない期間を表示します。
APN	アクセス ポイント名を表示します。

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	すべてのサービス ポリシー コンフィギュレーションをクリアします。
service-policy	サービス ポリシーを設定します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。

show shared license

共有ライセンス統計情報を表示するには、特権 EXEC モードで **show shared license** コマンドを使用します。オプションのキーワードはライセンス サーバのみで使用できます。

show shared license [**detail** | **client** [*hostname*] | **backup**]

構文の説明

バックアップ	(任意)バックアップ サーバに関する情報を表示します。
クライアント	(任意)参加ユニットの情報だけを表示します。
detail	(任意)参加ユニットごとの統計情報を含む、すべての統計情報を表示します。
hostname	(任意)特定の参加ユニットの情報だけを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

統計情報をクリアするには、**clear shared license** コマンドを入力します。

例

次に、ライセンス参加ユニットでの **show shared license** コマンドの出力例を示します。

```
ciscoasa# show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
```

```
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0

Client ID           Usage   Hostname
  ASA0926K04D         0       5510-B
```

表 12-3 に、**show shared license** コマンドの出力を示します。

表 12-3　show shared license の説明

フィールド	説明
Primary License Server	プライマリ サーバの IP アドレス。
Version	共有ライセンスのバージョン。
Status（ステータス）	コマンドがバックアップ サーバで発行された場合、「Active」はこのデバイスがプライマリ共有ライセンス サーバとしての役割を果たしていることを意味します。「Inactive」は、デバイスがスタンバイ モードで待機しており、デバイスはプライマリ サーバと通信していることを意味します。 フェールオーバー ライセンスがプライマリ サーバで設定されると、バックアップ サーバは、フェールオーバー中、瞬間的に「Active」になりますが、通信の同期が再び完了すると「Inactive」に戻ります。
Shared license utilization	
SSLVPN	
Total for network	使用可能な共有セッションの合計数が表示されます。
Available	使用できる残りの共有セッションを表示します。
Utilized	アクティブなライセンス サーバに対して取得された共有セッション数を表示します。
This device	
Platform limit	インストールされているライセンス応じて、デバイスの SSL VPN セッションの合計数を表示します。
現在の使用状況	現在このデバイスが所有する、共有プールからの共有 SSL VPN セッション数を表示します。
High usage	このデバイスが所有した共有 SSL VPN セッションの最大数を表示します。
Messages Tx/Rx/Error	
登録 get リリース Transfer	各接続タイプの送信、受信およびエラーのパケット数を示します。
Client ID	一意のクライアント ID。

表 12-3　show shared license の説明（続き）

フィールド	説明
使用法	使用中のセッション数を表示します。
Hostname	このデバイスのホスト名を表示します。

次に、ライセンス サーバ上での **show shared license detail** コマンドの出力例を示します。

```
ciscoasa# show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0

Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。

コマンド	説明
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

show shun

shun 情報を表示するには、特権 EXEC モードで **show shun** コマンドを使用します。

show shun [*src_ip* | *statistics*]

構文の説明

src_ip	(任意)このアドレスに関する情報を表示します。
statistics	(任意)インターフェイスのカウンタだけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

例

次に、**show shun** コマンドの出力例を示します。

```
ciscoasa# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

関連コマンド

コマンド	説明
clear shun	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
shun	新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。

show sip

SIP セッションを表示するには、特権 EXEC モードで **show sip** コマンドを使用します。

show sip

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show sip コマンドは、ASA を越えて確立されている SIP セッションの情報を表示します。

(注) **pager** コマンドを設定してから **show sip** コマンドを使用することを推奨します。多数の SIP セッション レコードが存在する場合に **pager** コマンドが設定されていないと、**show sip** コマンドが最後まで出力されるまでに時間がかかります。

例

次に、**show sip** コマンドの出力例を示します。

```
ciscoasa# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
|state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
|state Active, idle 0:00:06
```

この例では、ASA 上の 2 つのアクティブな SIP セッションが表示されています（`Total` フィールドを参照）。各 `call-id` が 1 つのコールを表します。

最初のセッションは call-id c3943000-960ca-2e43-228f@10.130.56.44 で、Call Init 状態にあります。これは、このセッションがまだコール設定中であることを示しています。コール設定が完了するのは、ACK が確認されてからです。このセッションは、1 秒間アイドル状態でした。

2 番めのセッションは Active 状態です。この状態ではコール設定が完了し、エンドポイントがメディアを交換しています。このセッションは、6 秒間アイドル状態でした。

関連コマンド

コマンド	説明
inspect sip	SIP アプリケーション インスペクションをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show skinny

SCCP（Skinny）インスペクション エンジンの問題をトラブルシューティングするには、特権 EXEC モードで **show skinny** コマンドを使用します。

show skinny

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show skinny コマンドは、SCCP（Skinny）セッションに関する情報を表示します。

例

次の条件での **show skinny** コマンドの出力例を示します。ASA を越えて 2 つのアクティブな Skinny セッションがセットアップされています。最初の Skinny セッションは、ローカル アドレス 10.0.0.11 にある内部 Cisco IP Phone と 172.18.1.33 にある外部 Cisco CallManager の間に確立されています。TCP ポート 2000 は、CallManager です。2 番目の Skinny セッションは、ローカル アドレス 10.0.0.22 にある別の内部 Cisco IP Phone と同じ Cisco CallManager の間に確立されています。

```
ciscoasa# show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                   FOREIGN                 STATE
-------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

この出力から、両方の内部 Cisco IP Phone の間でコールが確立されていることがわかります。最初と 2 番目の電話機の RTP リスン ポートは、それぞれ UDP 22948 と 20798 です。

関連コマンド

コマンド	説明
inspect skinny	SCCP アプリケーション インスペクションをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show sla monitor configuration

デフォルトを含む、SLA 動作のコンフィギュレーション値を表示するには、ユーザ EXEC モードで **show sla monitor configuration** コマンドを使用します。

show sla monitor configuration [*sla-id*]

構文の説明

sla-id	（任意）SLA 動作の ID 番号。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合は、すべての SLA 動作のコンフィギュレーション値が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

実行コンフィギュレーションの SLA 動作コマンドを確認するには、**show running config sla monitor** コマンドを使用します。

例

次に、**show sla monitor** コマンドの出力例を示します。SLA 動作 123 のコンフィギュレーション値が表示されます。**show sla monitor** コマンドの出力に続いて、同じ SLA 動作の **show running-config sla monitor** コマンドが出力されます。

```
ciscoasa> show sla monitor 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
```

```
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ciscoasa# show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーションの SLA 動作コンフィギュレーション コマンドを表示します。
sla monitor	SLA モニタリング動作を定義します。

show sla monitor operational-state

SLA 動作の動作状態を表示するには、ユーザ EXEC モードで **show sla monitor operational-state** コマンドを使用します。

show sla monitor operational-state [*sla-id*]

構文の説明

sla-id	（任意）SLA 動作の ID 番号。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合は、すべての SLA 動作の統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

実行コンフィギュレーションの SLA 動作コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次に、**show sla monitor operational-state** コマンドの出力例を示します。

```
ciscoasa> show sla monitor operation1-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
```

```
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーションの SLA 動作コンフィギュレーション コマンドを表示します。
sla monitor	SLA モニタリング動作を定義します。

show snmp-server engineid

ASA 上で設定されている SNMP エンジンの ID を表示するには、特権 EXEC モードで **show snmp-server engineid** コマンドを使用します。

show snmp-server engineid

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、**show snmp-server engineid** コマンドの出力例を示します。

```
ciscoasa# show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

使用上のガイドライン

SNMP エンジンは、ローカル デバイス上に配置できる SNMP のコピーです。エンジン ID は、各 ASA コンテキストの SNMP エージェントごとに割り当てられる固有の値です。ASA ではエンジン ID を設定できません。エンジン ID の長さは 25 バイトで、この ID は暗号化されたパスワードの生成に使用されます。暗号化されたパスワードはフラッシュ メモリに保存されます。エンジン ID はキャッシュすることができます。フェールオーバー ペアでは、エンジン ID がピアと同期化されます。

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
show running-config snmp-server	SNMP サーバ コンフィギュレーションを表示します。
snmp-server	SNMP サーバを設定します。

show snmp-server group

設定済みの SNMP グループの名前、使用するセキュリティ モデル、さまざまなビューのステータス、および各グループのストレージ タイプを表示するには、特権 EXEC モードで **show snmp-server group** コマンドを使用します。

show snmp-server group

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、**show snmp-server group** コマンドの出力例を示します。

```
ciscoasa# show snmp-server group
groupname: public                              security model:v1
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                              security model:v2c
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                    security model:v3 priv
readview : def_read_view                writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

使用上のガイドライン

SNMP ユーザおよび SNMP グループは、SNMP の View-based Access Control Model（VACM）に従って使用されます。使用されるセキュリティ モデルは、SNMP グループによって決まります。SNMP ユーザは、SNMP グループのセキュリティ モデルに一致する必要があります。各 SNMP グループ名とセキュリティ レベルのペアは一意である必要があります。

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
show running-config snmp-server	SNMP サーバ コンフィギュレーションを表示します。
snmp-server	SNMP サーバを設定します。

show snmp-server host

ホスト グループに属する設定済みの SNMP ホストの名前、使用されているインターフェイスおよび使用されている SNMP のバージョンを表示するには、特権 EXEC モードで **show snmp-server host** コマンドを使用します。

show snmp-server host

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.4(1)	出力は、ASA をポーリングしているアクティブなホストと、静的に設定されているホストのみを表示するように更新されました。

例

次に、**show snmp-server host** コマンドの出力例を示します。

```
ciscoasa# show snmp-server host
host ip = 10.10.10.1, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.10, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.2, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.4, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.5, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.7, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.8, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.9, interface = mgmt  poll community ***** version 2c
```

次に、Version 9.4(1) 現在の **show snmp-server host** コマンドの出力例を示します。ASA をポーリングしているアクティブなホストのみが表示されます。

```
ciscoasa# show snmp-server host
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
show running-config snmp-server	SNMP サーバ コンフィギュレーションを表示します。
snmp-server	SNMP サーバを設定します。

show snmp-server statistics

SNMP サーバ統計情報を表示するには、特権 EXEC モードで **show snmp-server statistics** コマンドを使用します。

show snmp-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show snmp-server statistics** コマンドの出力例を示します。

```
ciscoasa# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
clear snmp-server statistics	SNMP パケットの入力カウンタおよび出力カウンタをクリアします。
show running-config snmp-server	SNMP サーバ コンフィギュレーションを表示します。
snmp-server	SNMP サーバを設定します。

show snmp-server user

設定されている SNMP ユーザの特性に関する情報を表示するには、特権 EXEC モードで **show snmp-server user** コマンドを使用します。

show snmp-server user [*username*]

構文の説明

username	（任意）SNMP 情報を表示する特定のユーザ（複数可）を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、**show snmp-server user** コマンドの出力例を示します。

```
ciscoasa# show snmp-server user authuser
User name: authuser
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

この出力には次の情報が表示されます。

- ユーザ名。SNMP ユーザの名前を識別するストリングです。
- エンジン ID。ASA 上の SNMP のコピーを識別するストリングです。
- ストレージ タイプ。ASA の揮発性メモリまたは一時メモリに設定が格納されているか、あるいは不揮発性メモリまたは永続メモリに格納されているかを示します。非揮発性メモリまたは永続メモリに格納されている場合、ASA をオフにして再度オンにした場合でも設定は存続します。
- アクティブなアクセス リスト。SNMP ユーザに関連付けられている標準の IP アクセス リストです。

- Rowstatus。ユーザがアクティブか非アクティブかを示します。
- 認証プロトコル。使用されている認証プロトコルを示します。選択できるのは、MD5、SHA、なしのいずれかです。ソフトウェア イメージで認証がサポートされていない場合、このフィールドは表示されません。
- プライバシー プロトコル。DES によるパケット暗号化がイネーブルかどうかを示します。ソフトウェア イメージでプライバシーがサポートされていない場合、このフィールドは表示されません。
- グループ名。ユーザが属している SNMP グループを示します。SNMP グループは、View-based Access Control Model（VACM）に従って定義されます。

使用上のガイドライン

SNMP ユーザは、SNMP グループの一部である必要があります。*username* 引数が入力されなかった場合、**show snmp-server user** コマンドには設定済みのすべてのユーザに関する情報が表示されます。*username* 引数が入力され、そのユーザが存在する場合は、指定したユーザに関する情報が表示されます。

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
show running-config snmp-server	SNMP サーバ コンフィギュレーションを表示します。
snmp-server	SNMP サーバを設定します。

show software authenticity development

開発キー署名イメージのロードが有効または無効になっていることを確認するには、特権 EXEC モードで **show software authenticity development** コマンドを使用します。

show software authenticity development

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show software authenticity file** コマンドの出力例を示します。

```
ciscoasa(config)# show software authenticity development
Loading of development images is disabled
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show version	ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示します。
software authenticity key add special	SPI フラッシュに新しい開発キーを追加します。
software authenticity key revoke special	SPI フラッシュから古い開発キーを削除します。
show software authenticity keys	SPI フラッシュの開発キーを表示します。
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。

コマンド	説明
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。
show software authenticity	特定のイメージ ファイルのソフトウェア認証に関連したデジタル署名情報を表示します。

show software authenticity file

特定のイメージ ファイルのソフトウェア認証に関連したデジタル署名情報を表示するには、特権 EXEC モードで **show software authenticity file** コマンドを使用します。

show software authenticity [*filename*]

構文の説明

filename	(オプション)特定のイメージ ファイルを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show software authenticity file** コマンドの出力例を示します。

```
ciscoasa# show software authenticity file asa913.SSA
File Name                     : disk0:/asa913.SSA
Image type                    : Development
    Signer Information
        Common Name           : Cisco
        Organization Unit     : ASA5585-X
        Organization Name     : Engineering
    Certificate Serial Number : abcd1234efgh5678
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

この出力には次の情報が表示されます。

- メモリ内のファイルの名前であるファイル名。
- 表示されるイメージのタイプであるイメージ タイプ。
- 署名者情報によって、次のようなシグニチャ情報が指定されます。
  - 一般名。ソフトウェア メーカーの名前です。
  - 組織単位。ソフトウェア イメージが展開されるハードウェアを示します。
  - 組織名。ソフトウェア イメージの所有者です。

- 証明書シリアル番号。デジタル署名の証明書シリアル番号です。
- ハッシュ アルゴリズム。デジタル署名確認に使用されるハッシュ アルゴリズムのタイプを示します。
- 署名アルゴリズム。デジタル署名確認に使用される署名アルゴリズムのタイプを識別します。
- キー バージョン。確認に使用されるキー バージョンを示します。

関連コマンド

コマンド	説明
show version	ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示します。

show software authenticity keys

SPI フラッシュに格納されている開発キーおよびリリース キーの情報を表示するには、特権 EXEC モードで **show software authenticity keys** コマンドを使用します。

show software authenticity keys

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show software authenticity keys** コマンドの出力例を示します。

```
ciscoasa# show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
```

```
Exponent              : 65537
Key Version           : A
Public Key #2 Information
--------------------------
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #3 Information
--------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

関連コマンド

コマンド	説明
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
show software authenticity keys	開発キーを表示します。
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。

コマンド	説明
software authenticity key add special	SPR フラッシュに新しい開発キーを追加します。
software authenticity key revoke special	SPR フラッシュから古い開発キーを削除します。

show software authenticity running

特定のイメージ ファイルのソフトウェア認証に関連したデジタル署名情報を表示するには、特権 EXEC モードで **show software authenticity running** コマンドを使用します。このコマンドは、現在実行中のファイルに関連したデジタル署名情報を表示することを除き、**show software authenticity file** と同じです。

show software authenticity running

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show software authenticity running** コマンドの出力例を示します。

```
ciscoasa# show software authenticity running
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 5448091A
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : Cisco Systems ROMMON,1.0.16
```

この出力には次の情報が表示されます。

- メモリ内のファイルの名前であるファイル名。
- 表示されるイメージのタイプであるイメージ タイプ。

- 署名者情報によって、次のようなシグニチャ情報が指定されます。
  - 一般名。ソフトウェア メーカーの名前です。
  - 組織単位。ソフトウェア イメージが展開されるハードウェアを示します。
  - 組織名。ソフトウェア イメージの所有者です。
- 証明書シリアル番号。デジタル署名の証明書シリアル番号です。
- ハッシュ アルゴリズム。デジタル署名確認に使用されるハッシュ アルゴリズムのタイプを示します。
- 署名アルゴリズム。デジタル署名確認に使用される署名アルゴリズムのタイプを識別します。
- キー バージョン。確認に使用されるキー バージョンを示します。

関連コマンド

コマンド	説明
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
software authenticity key add special	SPR フラッシュに新しい開発キーを追加します。
software authenticity key revoke special	SPR フラッシュから古い開発キーを削除します。

show ssh sessions

ASA 上のアクティブな SSH セッションに関する情報を表示するには、特権 EXEC モードで **show ssh sessions** コマンドを使用します。

show ssh sessions [**hostname** or **A.B.C.D**] [**hostname** or **X:X:X:X::X**] [**detail**]

構文の説明

hostname or **A.B.C.D**	（オプション）指定された SSH クライアント IPv4 アドレスのみの SSH セッション情報を表示します。
hostname or **X:X:X:X::X**	（オプション）指定された SSH クライアント IPv6 アドレスのみの SSH セッション情報を表示します。
detail	SSH セッションの詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(2)	**detail** オプションが追加されました。

使用上のガイドライン

SID は、SSH セッションを識別する一意の番号です。Client IP は、SSH クライアントを実行しているシステムの IP アドレスです。Version は、SSH クライアントがサポートしているプロトコル バージョン番号です。SSH が SSH バージョン 1 だけをサポートしている場合、Version 列には 1.5 が表示されます。SSH クライアントが SSH バージョン 1 と SSH バージョン 2 の両方をサポートしている場合、Version 列には 1.99 が表示されます。SSH クライアントが SSH バージョン 2 だけをサポートしている場合、Version 列には 2.0 が表示されます。Encryption 列には、SSH クライアントが使用している暗号化のタイプが表示されます。State 列には、クライアントと ASA が行っている通信の進行状況が表示されます。Username には、このセッションで認証されているログイン ユーザ名が表示されます。Mode 列には、SSH データ ストリームの方向が表示されます。

SSH バージョン 2 の場合は、同じ暗号化アルゴリズムを使用することも、異なるアルゴリズムを使用することもできます。Mode フィールドには in および out が表示されます。SSH バージョン 1 の場合は、いずれの方向にも同じ暗号化を使用します。Mode フィールドには該当なしを表す記号（「-」）が表示され、1 つの接続に対して 1 つのエントリのみが表示されます。

例

次に、**show ssh sessions** コマンドの出力例を示します。

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

次に、**show ssh sessions detail** コマンドの出力例を示します。

```
ciscoasa# show ssh sessions detail
SSH Session ID              : 0
>   Client IP               : 161.44.66.200
>   Username                : root
>   SSH Version             : 2.0
>   State                   : SessionStarted
>   Inbound Statistics
>    Encryption             : aes256-cbc
>    HMAC                   : sha1
>    Bytes Received         : 2224
>   Outbound Statistics
>    Encryption             : aes256-cbc
>    HMAC                   : sha1
>    Bytes Transmitted      : 2856
>   Rekey Information
>    Time Remaining (sec)   : 3297
>    Data Remaining (bytes): 996145356
>    Last Rekey             : 16:17:19.732 EST Wed Jan 2 2013
>    Data-Based Rekeys      : 0
>    Time-Based Rekeys      : 0
```

関連コマンド

コマンド	説明
ssh disconnect	アクティブな SSH セッションを切断します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

show ssl

ASA 上の SSL 設定およびアクティブな SSL セッションに関する情報を表示するには、特権 EXEC モードで **show ssl** コマンドを使用します。

show ssl [**cache** | **ciphers** [*level*] | **errors** | **information** | **mib** | **objects**]

構文の説明

cache	（オプション）SSL セッション キャッシュの統計情報を表示します。
ciphers [*level*]	（オプション）**ssl cipher** コマンドを使用して設定したレベルに基づき、使用するために設定されている暗号方式を表示します。次のいずれかのレベルを指定すると、そのレベルの暗号方式のみを表示できます。レベルを指定しない場合、中間レベルの SSL、TLS、DTLS の各バージョンが表示されます。 • **all**：すべての暗号方式が含まれます。 • **low**：NULL-SHA を除くすべての暗号が含まれます。 • **medium**：NULL、DES、RC4 の暗号方式を除くすべての暗号方式が含まれます。 • **fips**：すべての FIPS 準拠の暗号方式が含まれます。 • **high**：TLSv1.2 にのみ適用され、最も強力な暗号方式のみが含まれます。
errors	（オプション）SSL エラーを表示します。
情報	（オプション）3DES ライセンスの有無にかかわらず、またデバイスでサポート可能なすべての暗号方式を使用して、SSL でサポートされている設定を表示します。
mib	（オプション）SSL MIB の統計情報を表示します。
オブジェクト	（オプション）SSL オブジェクトの統計情報を表示します。

デフォルト

Show ssl information では、次のデフォルト設定が 3DES の有無にかかわらず適用されます。

- 3DES（またはそれ以上の暗号サポート）がない場合のデフォルト設定は次のとおりです。

```
ssl server-version tlsv1 dtlsv1
ssl client-version tlsv1
ssl cipher default low
ssl cipher tlsv1 low
ssl cipher tlsv1.1 low
ssl cipher tlsv1.2 low
ssl cipher dtlsv1 low
ssl cipher dtlsv1.2 low
ssl dh-group group2
ssl ecdh-group group19
ssl certificate-authentication fca-timeout 2
```

- 3DES（またはそれ以上の暗号サポート）がある場合のデフォルト設定は次のとおりです。

```
ssl server-version tlsv1 dtlsv1
ssl client-version tlsv1 dtlsv1
ssl cipher default medium
ssl cipher tlsv1 medium
ssl cipher tlsv1.1 medium
ssl cipher tlsv1.2 medium
```

```
ssl cipher dtlsv1 medium
ssl cipher dtlsv1.2 medium
ssl dh-group group2
ssl ecdh-group group19
ssl certificate-authentication fca-timeout 2
```

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.1(2)	**detail** オプションが追加されました。
9.3(2)	TLSv1.1 および TLSv1.2 のサポートが追加されました。**ciphers** キーワードが追加されました。
9.12(1)	Show ssl cipher all コマンドが削除されて廃止され、show ssl cipher information コマンドが追加されました。

使用上のガイドライン

このコマンドは、現在の SSLv2 および SSLv3 セッションに関する情報を表示します。情報には、イネーブルにされた暗号の順序、ディセーブルにされた暗号、使用されている SSL トラストポイント、証明書認証がイネーブルかどうか、などが含まれます。

例

次に、**show ssl** コマンドの出力例を示します。

```
ciscoasa# show ssl

Accept connections using SSLv2 or greater and negotiate to TLSv1.2 or greater
Start connections using SSLv3 and negotiate to SSLv3 or greater
SSL DH Group: group2

SSL trust-points:
  Self-signed RSA certificate available
  Default: certsha256
  Interface inside: certsha256
Certificate authentication is not enabled
```

次に、**show ssl ciphers fips** コマンドの出力例を示します。

```
ciscoasa# show ssl ciphers fips
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
```

```
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
```

次に、**show ssl ciphers** コマンドの出力を示します。

```
ciscoasa# show ssl ciphers all
These are the ciphers for the given cipher level; not all ciphers
are supported by all versions of SSL/TLS.
These names can be used to create a custom cipher list
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DES-CBC3-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  RC4-SHA (tlsv1)
  RC4-MD5 (tlsv1)
  DES-CBC-SHA (tlsv1)
  NULL-SHA (tlsv1)
asa3(config-tlsp)# show ssl ciphers medium
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
```

```
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
asa3(config-tlsp)# show ssl ciphers fips
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
asa3(config-tlsp)# show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
```

```
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
```

関連コマンド

コマンド	説明
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
ssl ciphers	SSL、DTLS、および TLS プロトコルの暗号化アルゴリズムを指定します。

show startup-config

スタートアップ コンフィギュレーションを表示したり、スタートアップ コンフィギュレーションがロードされたときのエラーを表示したりするには、特権 EXEC モードで **show startup-config** コマンドを使用します。

show startup-config [**errors**]

構文の説明

errors	(任意)ASA がスタートアップ コンフィギュレーションをロードしたときに生成されたエラーを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム[1]
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

1. **errors** キーワードは、シングル モードおよびシステム実行スペースでだけ使用できます。

コマンド履歴

リリース	変更内容
7.0(1)	**errors** キーワードが追加されました。
8.3(1)	暗号化されたパスワードが出力に追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、**show startup-config** コマンドは現在の実行スペース(システム コンフィギュレーションまたはセキュリティ コンテキスト)のスタートアップ コンフィギュレーションを表示します。

show startup-config コマンドの出力では、パスワードの暗号化が有効か無効かに応じて、パスワードが暗号化、マスク、またはクリア テキストの状態で表示されます。

スタートアップ エラーをメモリからクリアするには、**clear startup-config errors** コマンドを使用します。

例

次に、**show startup-config** コマンドの出力例を示します。

```
ciscoasa# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003
```

```
Version 7.X(X)
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 209.165.200.224
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 209.165.200.225
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 209.165.200.226
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

次に、**show startup-config errors** コマンドの出力例を示します。

```
ciscoasa# show startup-config errors

ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done. (1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', "nameif inside"
.....
*** Output from config line 37, "config-url disk:/admin..."
```

関連コマンド

コマンド	説明
clear startup-config errors	スタートアップ エラーをメモリからクリアします。
show running-config	実行コンフィギュレーションを表示します。

show sunrpc-server active

Sun RPC サービス用に開いているピンホールを表示するには、特権 EXEC モードで **show sunrpc-server active** コマンドを使用します。

show sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show sunrpc-server active コマンドは、NFS や NIS などの Sun RPC サービス用に開いているピンホールを表示するために使用します。

例

Sun RPC サービスで開かれているピンホールを表示するには、**show sunrpc-server active** コマンドを入力します。次に、**show sunrpc-server active** コマンドの出力例を示します。

```
ciscoasa# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

LOCAL カラムのエントリは、内部インターフェイスのクライアントまたはサーバの IP アドレスを示します。FOREIGN カラムの値は、外部インターフェイスのクライアントまたはサーバの IP アドレスを示します。

関連コマンド

コマンド	説明
clear configure sunrpc-server	ASA からの Sun リモート プロセッサ コール サービスをクリアします。
clear sunrpc-server active	NFS や NIS などの Sun RPC サービス用に開いているピンホールをクリアします。

コマンド	説明
inspect sunrpc	Sun RPC アプリケーション インスペクションをイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	SunRPC サービス コンフィギュレーションに関する情報を表示します。

show switch mac-address-table

スイッチの MAC アドレステーブルを表示するには、特権 EXEC モードで **show switch mac-address-table** コマンドを使用します。

show switch mac-address-table

(注) Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

スイッチ MAC アドレス テーブルには、スイッチ ハードウェア内の各 VLAN のトラフィックに適用する MAC アドレスとスイッチ ポートのマッピングが保持されます。トランスペアレント ファイアウォール モードでは、**show mac-address-table** コマンドを使用して ASA ソフトウェア内のブリッジ MAC アドレス テーブルを表示します。このブリッジ MAC アドレス テーブルには、VLAN 間を通過するトラフィックに適用する MAC アドレスと VLAN インターフェイスのマッピングが保持されます。

MAC アドレス エントリは 5 分経過するとエージング アウトします。

例

次に、**show switch mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |       Type        | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic       | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic       | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic       | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic       | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static        |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast  |  -  | In0/1,Et0/0-7
Total Entries: 6
```

表 12-4 に、各フィールドの説明を示します。

表 12-4　show switch mac-address-table のフィールド

フィールド	説明
Mac Address	MAC アドレスを表示します。
VLAN	MAC アドレスに関連付けられている VLAN を表示します。
タイプ	MAC アドレスを、ダイナミックに学習するか、スタティック マルチキャスト アドレスとして学習するか、またはスタティックに学習するかを示します。スタティック エントリは、内部バックプレーン インターフェイスの場合にのみ該当します。
Age	MAC アドレス テーブル内にあるダイナミック エントリの経過時間を表示します。
Port	この MAC アドレスのホストに到達できるスイッチ ポートを表示します。

関連コマンド

コマンド	説明
show mac-address-table	組み込みスイッチのないモデルの MAC アドレス テーブルを表示します。
show switch vlan	VLAN と物理 MAC アドレスの関連付けを表示します。

show switch vlan

VLAN および関連するスイッチポートを表示するには、特権 EXEC モードで **show switch vlan** コマンドを使用します。

show switch vlan

(注) Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

このコマンドは、組み込みスイッチを持つモデル専用です。他のモデルの場合は、**show vlan** コマンドを使用します。

例

次に、**show switch vlan** コマンドの出力例を示します。

```
ciscoasa# show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                            up        Et0/0, Et0/1
200  outside                           up        Et0/7
300  -                                 down      Et0/1, Et0/2
400  backup                            down      Et0/3
```

表 12-5 に、各フィールドの説明を示します。

表 12-5　show switch vlan のフィールド

フィールド	説明
VLAN	VLAN 番号を表示します。
名前	VLAN インターフェイスの名前を表示します。**nameif** コマンドを使用して名前が設定されていない場合、または **interface vlan** コマンドが実行されていない場合は、ダッシュ(-)が表示されます。
Status(ステータス)	スイッチ内の VLAN とトラフィックを送受信するためのステータス(up または down)を表示します。VLAN がアップ状態になるには、その VLAN で少なくとも 1 つのスイッチ ポートがアップ状態である必要があります。
ポート	各 VLAN に割り当てられたスイッチ ポートを表示します。1 つのスイッチ ポートが複数の VLAN にリストされている場合、そのポートはトランク ポートです。上記の出力例で、Ethernet 0/1 は VLAN 100 および VLAN 300 を伝送するトランク ポートです。

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show vlan	組み込みスイッチのないモデルの VLAN を表示します。
switchport mode	スイッチ ポートのモードをアクセス モードまたはトランク モードに設定します。

show sw-reset-button

ASA 5506-X、5508-X、または 5516-X のソフトウェア リセット ボタンが有効になっているかどうかを表示するには、特権 EXEC モードで **show sw-reset-button** コマンドを使用します。

show sw-reset-button

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ソフトウェア リセット ボタンはデフォルトで有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	コマンドが追加されました。

使用上のガイドライン

service sw-reset-button コマンドを使用して、ソフトウェア リセット ボタンを有効または無効にします。リセット ボタンは背面パネルにある小さな埋め込み型のボタンです。約 3 秒以上押すと ASA がリセットされ、次のリブート後に「出荷時」のデフォルト状態に戻ります。設定変数が工場出荷時デフォルトにリセットされます。ただし、フラッシュは削除されないため、ファイルは削除されません。

例

次に、ソフトウェア リセット ボタンをイネーブルにする例を示します。

```
ciscoasa(config)# service sw-reset-button
ciscoasa(config)# show sw-reset-button

Software Reset Button is configured.
```

次に、ソフトウェア リセット ボタンを無効にする例を示します。

```
ciscoasa(config)# no service sw-reset-button
ciscoasa(config)# show sw-reset-button

Software Reset Button is not configured.
```

関連コマンド

コマンド	説明
service sw-reset-button	ソフトウェア リセット ボタンをイネーブルまたはディセーブルにします。

show tcpstat コマンド～ show traffic コマンド

show tcpstat

ASA の TCP スタックおよび ASA で終端している TCP 接続のステータスを（デバッグのために）表示するには、特権 EXEC モードで **show tcpstat** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

show tcpstat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show tcpstat コマンドを使用すると、TCP スタックおよび ASA で終端している TCP 接続のステータスを表示できます。表 28 に、表示される TCP 統計情報の説明を示します。

表 13-1　show tcpstat コマンドの TCP 統計情報

統計	説明
tcb_cnt	TCP ユーザの数。
proxy_cnt	TCP プロキシの数。TCP プロキシは、ユーザ認可で使用されます。
tcp_xmt pkts	TCP スタックが送信したパケットの数。
tcp_rcv good pkts	TCP スタックが受信した正常なパケットの数。
tcp_rcv drop pkts	TCP スタックがドロップした受信パケットの数。
tcp bad chksum	チェックサムに誤りがあった受信パケットの数。
tcp user hash add	ハッシュ テーブルに追加された TCP ユーザの数。
tcp user hash add dup	新しい TCP ユーザをハッシュ テーブルに追加しようとしたとき、そのユーザがすでにテーブル内に存在していた回数。
tcp user srch hash hit	検索時にハッシュ テーブル内で TCP ユーザが検出された回数。
tcp user srch hash miss	検索時にハッシュ テーブル内で TCP ユーザが検出されなかった回数。
tcp user hash delete	TCP ユーザがハッシュ テーブルから削除された回数。
tcp user hash delete miss	TCP ユーザを削除しようとしたとき、そのユーザがハッシュ テーブル内で検出されなかった回数。
lip	TCP ユーザのローカル IP アドレス。
fip	TCP ユーザの外部 IP アドレス。
lp	TCP ユーザのローカル ポート。
fp	TCP ユーザの外部ポート。
st	TCP ユーザの状態（RFC 793 を参照）。表示される値は次のとおりです。 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	TCP ユーザの再送信キューの長さ。
inqlen	TCP ユーザの入力キューの長さ。
tw_timer	TCP ユーザの time_wait タイマーの値（ミリ秒）。
to_timer	TCP ユーザの非アクティビティ タイムアウト タイマーの値（ミリ秒）。
cl_timer	TCP ユーザのクローズ要求タイマーの値（ミリ秒）。
per_timer	TCP ユーザの持続タイマーの値（ミリ秒）。

表 13-1　show tcpstat コマンドの TCP 統計情報(続き)

統計	説明
rt_timer	TCP ユーザの再送信タイマーの値(ミリ秒)。
tries	TCP ユーザの再送信回数。

例

次に、ASA の TCP スタックのステータスを表示する例を示します。

```
ciscoasa# show tcpstat
                 CURRENT MAX      TOTAL
tcb_cnt          2       12       320
proxy_cnt        0       0        160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

関連コマンド

コマンド	説明
show conn	使用されている接続と使用可能な接続を表示します。

show tech-support

テクニカル サポート アナリストが診断時に使用する情報を表示するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support [**detail** [**vsn**] | **file** | **no-config** | **performance**]

構文の説明

detail	（任意）詳細情報を表示します。
file	（任意）コマンドの出力をファイルに書き込みます。ファイル システムのタイプは次のとおりです。disk0:、disk1:、ftp:、scp:、smb:、および tftp:。
no-config	（任意）実行コンフィギュレーションの出力を除外します。
パフォーマンス	（オプション）パフォーマンス情報を表示します。
vsn	（オプション）ファイルにリダイレクトされる追加の ASA1000V ポリシー エージェントのテクニカル サポート情報を含めます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	**detail** キーワードおよび **file** キーワードが追加されました。
7.2(1)	出力が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。
9.1(2)	出力が拡張され、**show environment** コマンドの情報が含まれるようになりました。
9.1(3)	出力が拡張され、**show memory detail**、**show memory top-usage**、および **show vlan** コマンドの情報が含まれるようになりました。
9.2(1)	**show memory detail**、**show cpu detail**、**show blocks queue history core-local**、**show asp drop**、**show asp event dp-cp**、**show cpu usage history** および **show traffic summary** コマンドからの情報を含むように出力が拡張されました。**show kernel cgroup-controller detail** コマンドからの出力は削除されました。**performance** および **vsn** キーワードが追加されました。
9.2(1)	出力が拡張され、**show vlan** コマンドの情報が含まれるようになりました。

リリース	変更内容
9.1(7)/9.3(1)	**show tech-support** コマンドに **show resource usage count all 1** の出力が含まれるようになりました。これには、xlate、conn、inspect、syslog などに関する情報が含まれます。この情報は、パフォーマンスに関する問題を診断するために役立ちます。
9.3(2)	**show route-summary** コマンドの出力が **show tech-support detail** コマンドに追加されました。
9.4(1)	**show tech-support** コマンドの出力には、生成された syslog の最新 50 行が含まれます。これらの結果を表示できるようにするには、**logging buffer** コマンドをイネーブルにする必要があります。
9.1(7)/9.4(3)/9.5(2)	**show tech support** コマンドは現在次のとおりです。 • **dir all-filesystems** の出力が含まれます。この出力は次の場合に役立つことがあります。 – SSL VPN コンフィギュレーション: 必要なリソースが ASA にあるかどうかを確認します。 – クラッシュ: クラッシュ ファイルの日付のタイムスタンプと存在を確認します。 • **show kernel cgroup-controller detail** の出力の削除: このコマンド出力は **show tech-support detail** の出力内に残されます。
9.7.(1)	**show tech-support** コマンドは、次の変更が加えられ更新されました。 • クラッシュしたスレッドからの **thread name**、**registry content**、**timestamp**、**traceback** などの crashinfo 統計情報を含むように出力が拡張されました。**Saved crash** のタイムスタンプからの出力は削除されました。 • **show ipsec stats**、**show crypto ikev1 stats** および **show crypto ikev2 stats** コマンドを含むように出力が拡張されました。これらのコマンドは、トラブルシューティングを目的として、VPN 統計情報を収集するために使用されます。 • **show tech-support** コマンドに、**show vm** の出力が含まれるようになりました。これは、ASAv が現在稼働しているハイパーバイザーを判別します。この情報は、仮想プラットフォーム上で複数の自動化されたチェックを実行するために役立ちます。 • **show tech-support** コマンドに **show module detail** コマンドが含まれるようになりました。このコマンドは、複数のモジュールに関する情報を提供するため、さまざまな接続およびステータスの問題のトラブルシューティングに役立ちます。
9.12(1)	**show ipv6 interface**、**show aaa server**、および **show fragment** の出力が **show tech support** の出力に追加されました。
9.13(1)	**show flow-offload info detail**、**show flow offload statistics**、および **show asp table socket** コマンドが追加されました。

使用上のガイドライン

show tech-support コマンドでは、テクニカル サポート アナリストが問題を診断する場合に役立つ情報が表示されます。テクニカル サポート アナリストは、このコマンドと各種 **show** コマンドの出力を組み合わせてさまざまな情報を入手します。

例

次に、テクニカル サポート分析に使用される情報を表示する例を示します。出力が、**show module** コマンドの出力で始まるように短縮されています。

```
ciscoasa# show tech-support | beg show module

------------------ show module ------------------

Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5525-X with SW, 8 GE Data, 1 GE Mgmt, AC ASA5525            FCH18087TA3
 ips Unknown                                     N/A                FCH18087TA3
cxsc Unknown                                     N/A                FCH18087TA3
 sfr Unknown                                     N/A                FCH18087TA3

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 7426.ac5a.b362 to 7426.ac5a.b36b  1.0          2.1(9)8      99.3(0)34
 ips 7426.ac5a.b360 to 7426.ac5a.b360  N/A          N/A
cxsc 7426.ac5a.b360 to 7426.ac5a.b360  N/A          N/A
 sfr 7426.ac5a.b360 to 7426.ac5a.b360  N/A          N/A

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 ips Unknown                        No Image Present Not Applicable
cxsc Unknown                        No Image Present Not Applicable
 sfr Unknown                        No Image Present Not Applicable

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
 ips Unresponsive       Not Applicable
cxsc Unresponsive       Not Applicable
 sfr Unresponsive       Not Applicable

Mod  License Name   License Status  Time Remaining
---- -------------- --------------- ---------------
 ips IPS Module     Disabled        perpetual


------------------ show inventory ------------------

Name: "Chassis", DESCR: "ASA 5525-X with SW, 8 GE Data, 1 GE Mgmt, AC"
PID: ASA5525           , VID: V02     , SN: FTX181010F5

Name: "Storage Device 1", DESCR: "Model Number: Micron_M550_MTFDDAK128MAY"
PID: N/A               , VID: N/A     , SN: MXA184200GL


------------------ show environment ------------------


Cooling Fans:
-------------------------------------

   Chassis Fans:
   --------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5888 RPM - OK
   Cooling Fan 3: 5888 RPM - OK

Temperature:
-------------------------------------
```

```
   Processors:
   --------------------------------
   Processor 1: 64.0 C - OK

   Chassis:
   --------------------------------
   Ambient 1: 45.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 40.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 46.0 C - OK  (Chassis Back Left Temperature)

Voltage:
---------------------------------
   Channel 1: 1.064 V - OK  (CPU Core)
   Channel 2: 12.126 V - OK  (12V)
   Channel 3: 5.104 V - OK  (5V)
   Channel 4: 3.280 V - OK  (3.3V)
   Channel 5: 1.504 V - OK  (DDR3 1.5V)
   Channel 6: 1.048 V - OK  (PCH 1.05V)

ALARM CONTACT 1
    Status:      not asserted
    Description: external alarm contact 1
    Severity:    minor
    Trigger:     closed

ALARM CONTACT 2
    Status:      not asserted
    Description: external alarm contact 2
    Severity:    minor
    Trigger:     closed

Driver Information:
--------------------
Status : RUNNING

Driver Error Statistics:
-------------------------
I2C I/O Errors          : 0
GPIO Errors             : 0
Ioctl Null Ptr Errors   : 0
Poll Errors             : 0
Invalid Ioctl Errors    : 1
PECI Errors             : 0
Unknown Errors          : 0

Last 5 Errors:
---------------

------------------ show memory ------------------

Free memory:        3512376646 bytes (80%)
Used memory:         868110256 bytes (20%)
-------------     ------------------
Total memory:       4380486902 bytes (100%)

Note: Free memory is the free system memory. Additional memory may
      be available from memory pools internal to the firewall process.
      Use 'show memory detail' to see this information, but use it
      with care since it may cause CPU hogs and packet loss under load.

------------------ show memory detail ------------------
```

```
Heap Memory:
   Free Memory:
      Heapcache Pool:                      376278288 bytes (  9% )
      Global Shared Pool:                     134208 bytes (  0% )
      Message Layer Pool:                    1980160 bytes (  0% )
      System:                             3133648118 bytes ( 72% )
   Used Memory:
      Heapcache Pool:                      313684720 bytes (  7% )
      Global Shared Pool:                        960 bytes (  0% )
      Reserved (Size of DMA Pool):         230686720 bytes (  5% )
      Reserved for messaging:                 116992 bytes (  0% )
      MMAP usage:                            7782400 bytes (  0% )
      System Overhead:                     316174336 bytes (  7% )
-----------------------------------     ----------------
   Total Memory:                       4380486902 bytes ( 100% )

Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.

------------------------------------------------------------------------
MEMPOOL_MSGLYR POOL STATS:

Non-mmapped bytes allocated =      2097152
Number of free chunks       =            6
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =      2097152
Keepcost                    =      1979264
Max contiguous free mem     =      1979264
Allocated memory in use     =       116992
Free memory                 =      1980160

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           48             1             48
           64             1             64
           96             1             96**
          112             1            112
          144             1            144
      1979264             1        1979264*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           80            19           1520
           96            11           1056
          112            23           2576
          128            21           2688
          144             3            432
          160             2            320
          176             6           1056
          192             5            960
          208             2            416
          224             4            896
          240             6           1440
```

```
          256             4           1024
          384            11           4224
          512             6           3072
          768             3           2304
         1024             6           6144
         4096             1           4096
         8192             9          73728

MEMPOOL_HEAPCACHE_0 POOL STATS:

Non-mmapped bytes allocated =    689963008
Number of free chunks       =          562
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    689963008
Keepcost                    =    331991792
Max contiguous free mem     =    331991792
Allocated memory in use     =    313684720
Free memory                 =    376278288

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           32           232            7424
           48           147            7056
           64           165           10560
           80             1              80
           96             1              96**
           96             1              96
          128             1             128
          160             2             320
          176             3             528
          512             1             560
       393216             1          404208
       524288             1          636784
      4194304             1         4730464
      6291456             3        20478336
     12582912             1        17731296
    331991792             1       331991792*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
----------------  ----------  --------------
           80          1518          121440
           96         12863         1234848
          112          3021          338352
          128          1643          210304
          144          3359          483696
          160           422           67520
          176           392           68992
          192           360           69120
          208           263           54704
          224           276           61824
          240           187           44880
          256          2564          656384
          384           549          210816
```

```
          512           837         428544
          768           729         559872
         1024           747         764928
         1536           343         526848
         2048           371         759808
         3072            49         150528
         4096           426        1744896
         6144            59         362496
         8192           205        1679360
        12288           114        1400832
        16384           593        9715712
        24576            24         589824
        32768            68        2228224
        49152            19         933888
        65536           424       27787264
        98304            21        2064384
       131072            15        1966080
       196608            15        2949120
       262144            17        4456448
       393216            16        6291456
       524288            12        6291456
       786432             4        3145728
      1048576            17       17825792
      1572864             5        7864320
      2097152             5       10485760
      3145728             1        3145728
      4194304             3       12582912
      6291456             4       25165824
      8388608             1        8388608
     12582912             4       50331648

MEMPOOL_DMA POOL STATS:

Non-mmapped bytes allocated =    230686720
Number of free chunks       =          156
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    230686720
Keepcost                    =     41968336
Max contiguous free mem     =     41968336
Allocated memory in use     =    188644800
Free memory                 =     42041920

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           96             1             96**
          256            60          19328
          384            32          15360
          512            62          38688
     41968336             1       41968336*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
          160             2            320
```

```
          256             7           1792
          384             1            384
          512             3           1536
          768             5           3840
         1024           164         167936
         2048             6          12288
         8192             1           8192
        12288            18         221184
        16384             1          16384
        32768             7         229376
        49152             3         147456
        65536             1          65536
        98304             4         393216
       131072             4         524288
       196608             6        1179648
       262144             4        1048576
       393216             6        2359296
       524288            10        5242880
       786432             2        1572864
      1048576             3        3145728
      1572864             6        9437184
      2097152             4        8388608
      3145728             7       22020096
      6291456             2       12582912
     12582912             3       37748736

MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =       135168
Number of free chunks       =            3
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =            0
Keepcost                    =        97136
Max contiguous free mem     =            0
Allocated memory in use     =          960
Free memory                 =       134208

----- fragmented memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           80             1             80
          112           329          36848
          144             1            144

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                       (bytes)
---------------  ----------  --------------
           88             1             88
          104             1            104
          168             1            168
          184             3            552

Summary for all pools:

Non-mmapped bytes allocated =    922882048
Number of free chunks       =          727
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    922746880
```

```
Keepcost                    =    376036528
Allocated memory in use     =    502447472
Free memory                 =    420434576


------------------ show conn count ------------------

1 in use, 18 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show vpn-sessiondb summary ------------------

--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ------------------------------------------------
OSPFv3 IPsec                :      1 :          1 :           1
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :      1
Device Total VPN Capacity   :    750
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
IPsec                       :      1 :          1 :               1
--------------------------------------------------------------------------------
Totals                      :      1 :          1
--------------------------------------------------------------------------------

------------------ show aaa-server ------------------

Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at unknown
Number of pending requests              0
Average round trip time                 0ms
Number of authentication requests       0
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       0
Number of rejects                       0
Number of challenges                    0
Number of malformed responses           0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0

Server Group:    ACS
Server Protocol: radius
Server Address:  65.5.31.100
Server port:     1645(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at unknown
Number of pending requests              0
```

```
Average round trip time                 0ms
Number of authentication requests       0
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       0
Number of rejects                       0
Number of challenges                    0
Number of malformed responses           0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0

------------------ show ipsec stats ------------------


IPsec Global Statistics
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 0
    Decompressed bytes: 0
    Packets: 0
    Dropped packets: 0
    Replay failures: 0
    Authentications: 0
    Authentication failures: 0
    Decryptions: 0
    Decryption failures: 0
    TFC Packets: 0
    Decapsulated fragments needing reassembly: 0
    Valid ICMP Errors rcvd: 0
    Invalid ICMP Errors rcvd: 0
Outbound
    Bytes: 0
    Uncompressed bytes: 0
    Packets: 0
    Dropped packets: 0
    Authentications: 0
    Authentication failures: 0
    Encryptions: 0
    Encryption failures: 0
    TFC Packets: 0
    Fragmentation successes: 0
        Pre-fragmentation successses: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
Inbound SA delete requests: 0
Outbound SA delete requests: 0
Inbound SA destroy calls: 0
Outbound SA destroy calls: 0
```

```
------------------ show crypto ikev1 stats ------------------


Global IKEv1 Statistics
  Active Tunnels:              0
  Previous Tunnels:            0
  In Octets:                   0
  In Packets:                  0
  In Drop Packets:             0
  In Notifys:                  0
  In P2 Exchanges:             0
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    0
  Out Octets:                  0
  Out Packets:                 0
  Out Drop Packets:            0
  Out Notifys:                 0
  Out P2 Exchanges:            0
  Out P2 Exchange Invalids:    0
  Out P2 Exchange Rejects:     0
  Out P2 Sa Delete Requests:   0
  Initiator Tunnels:           0
  Initiator Fails:             0
  Responder Fails:             0
  System Capacity Fails:       0
  Auth Fails:                  0
  Decrypt Fails:               0
  Hash Valid Fails:            0
  No Sa Fails:                 0

------------------ show crypto ikev2 stats ------------------


Global IKEv2 Statistics
Active Tunnels: 0
Previous Tunnels: 0
In Octets: 0
In Packets: 0
In Drop Packets: 0
In Drop Fragments: 0
In Notifys: 0
In Child SA Exchanges: 0
In Child SA Exchange Invalids: 0
In Child SA Exchange Rejects: 0
In Child SA Sa Delete Requests: 0
Out Octets: 0
Out Packets: 0
Out Drop Packets: 0
Out Drop Fragments: 0
Out Notifys: 0
Out Child SA Exchanges: 0
Out Child SA Exchange Invalids: 0
Out Child SA Exchange Rejects: 0
Out Child SA Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
```

```
------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     0   2950   2939   2950
     4    400    399    399
    80   2500   2459   2500
   256   5660   5544   5655
  1550  10589  10580  10587
  2048   8848   8848   8848
  2560   2964   2964   2964
  4096    100    100    100
  8192    100    100    100
  9344    100    100    100
 16384    154    154    154
 65536     16     16     16

------------------ show blocks core ------------------

CORE  LIMIT  ALLOC   HIGH    CNT       FAILED
   0  24576     16     16     16            0

------------------ show blocks queue history detail ------------------

History buffer memory usage: 3744 bytes (default)
History analysis time limit: 100 msec

Please see 'show blocks exhaustion snapshot' for more information

------------------ show blocks queue history core-local ------------------

History buffer memory usage: 3744 bytes (default)
History analysis time limit: 100 msec

------------------ show interface ------------------

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address 7426.ac5a.b367, MTU 1500
        IP address 85.5.28.254, subnet mask 255.255.224.0
        60 packets input, 4786 bytes, 0 no buffer
        Received 34 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        47 packets output, 4232 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (501/461)
        output queue (blocks free curr/low): hardware (511/508)
  Traffic Statistics for "outside":
        60 packets input, 3706 bytes
        47 packets output, 3296 bytes
        2 packets dropped
      1 minute input rate 0 pkts/sec,  2 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  2 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

```
  Control Point Interface States:
        Interface number is 3
        Interface config status is active
        Interface state is active
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address 7426.ac5a.b363, MTU 1500
        IP address 65.5.28.254, subnet mask 255.255.224.0
        34 packets input, 2748 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        79 packets output, 6280 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (477/477)
        output queue (blocks free curr/low): hardware (511/508)
  Traffic Statistics for "inside":
        34 packets input, 2136 bytes
        79 packets output, 4192 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 4
        Interface config status is active
        Interface state is active
Interface GigabitEthernet0/2 "82net", is administratively down, line protocol is down
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address 7426.ac5a.b368, MTU 1500
        IP address 82.124.22.9, subnet mask 255.252.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Traffic Statistics for "82net":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

```
  Control Point Interface States:
        Interface number is 5
        Interface config status is not active
        Interface state is not active
Interface GigabitEthernet0/2.83 "83net", is down, line protocol is down
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 83
        MAC address 7426.ac5a.b368, MTU 1500
        IP address 83.124.22.9, subnet mask 255.252.0.0
  Control Point Interface States:
        Interface number is 16
        Interface config status is active
        Interface state is not active
  Control Point Vlan83 States:
        Interface vlan config status is active
        Interface vlan state is DOWN
Interface GigabitEthernet0/3 "failover", is down, line protocol is down
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Description: LAN/STATE Failover Interface
        MAC address 7426.ac5a.b364, MTU 1500
        IP address 99.1.1.1, subnet mask 255.255.255.0
        454 packets input, 107664 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        457 packets output, 45112 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Traffic Statistics for "failover":
        403 packets input, 81258 bytes
        397 packets output, 31420 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 6
        Interface config status is active
        Interface state is not active
Interface GigabitEthernet0/4 "", is administratively down, line protocol is down
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address 7426.ac5a.b369, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
```

```
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Control Point Interface States:
        Interface number is 7
        Interface config status is not active
        Interface state is not active
Interface GigabitEthernet0/5 "", is administratively down, line protocol is down
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address 7426.ac5a.b365, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Control Point Interface States:
        Interface number is 8
        Interface config status is not active
        Interface state is not active
Interface GigabitEthernet0/6 "", is administratively down, line protocol is down
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address 7426.ac5a.b36a, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Control Point Interface States:
        Interface number is 9
        Interface config status is not active
        Interface state is not active
Interface GigabitEthernet0/7 "", is administratively down, line protocol is down
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address 7426.ac5a.b366, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Control Point Interface States:
        Interface number is 10
        Interface config status is not active
        Interface state is not active
Interface Internal-Control0/0 "cplane", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.0001.0001, MTU 1500
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        796 packets output, 43320 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "cplane":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 12
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "asa_mgmt_plane", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        (Full-duplex), (100 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address 7426.ac5a.b362, MTU not set
        IP address unassigned
        8925 packets input, 720821 bytes, 0 no buffer
        Received 8677 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        4081 packets output, 1010626 bytes, 825 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 1 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (505/459)
        output queue (blocks free curr/low): hardware (460/0)
```

```
  Traffic Statistics for "asa_mgmt_plane":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active
Interface Internal-Data0/1 "", is down, line protocol is down
  Hardware is ivshmem rev03, BW 1000 Mbps, DLY 10 usec
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 output decode drops
        0 input reset drops, 0 output reset drops
        Queue Stats:
          RX[00]: 0 packets, 0 bytes, 0 overrun
                  Blocks free curr/low: -1/2687
          RX[01]: 0 packets, 0 bytes, 0 overrun
                  Blocks free curr/low: -1/2687
          RX[02]: 0 packets, 0 bytes, 0 overrun
                  Blocks free curr/low: -1/2687
          TX[00]: 0 packets, 0 bytes, 0 underruns
                  Blocks free curr/low: -1/2687
          TX[01]: 0 packets, 0 bytes, 0 underruns
                  Blocks free curr/low: -1/2687
          TX[02]: 0 packets, 0 bytes, 0 underruns
                  Blocks free curr/low: -1/2687
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
Interface Internal-Data0/2 "mgmt_plane_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.0001.0003, MTU not set
        IP address unassigned
        4907 packets input, 1213857 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        8985 packets output, 689313 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
```

```
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "mgmt_plane_int_tap":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 13
        Interface config status is active
        Interface state is active
Interface Internal-Data0/3 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.0100.0001, MTU 1500
        IP address 169.254.1.1, subnet mask 255.255.255.248
        8 packets input, 676 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        5 packets output, 370 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
        8 packets input, 564 bytes
        5 packets output, 300 bytes
        8 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 15
        Interface config status is active
        Interface state is active
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address 7426.ac5a.b362, MTU 1500
        IP address 10.86.193.25, subnet mask 255.255.255.192
        9048 packets input, 693653 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        4896 packets output, 1212963 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 1 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
```

```
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "management":
        9048 packets input, 549861 bytes
        4896 packets output, 1144419 bytes
        3256 packets dropped
      1 minute input rate 15 pkts/sec,  865 bytes/sec
      1 minute output rate 0 pkts/sec,  40 bytes/sec
      1 minute drop rate, 4 pkts/sec
      5 minute input rate 12 pkts/sec,  766 bytes/sec
      5 minute output rate 0 pkts/sec,  44 bytes/sec
      5 minute drop rate, 4 pkts/sec
        Management-only interface. Blocked 0 through-the-device packets
                0 IPv4 packets originated from management network
                0 IPv4 packets destined to management network
                0 IPv6 packets originated from management network
                0 IPv6 packets destined to management network
  Control Point Interface States:
        Interface number is 14
        Interface config status is active
        Interface state is active

------------------ show ipv6 interface ------------------

82net is administratively down, line protocol is down
  IPv6 is enabled, link-local address is fe80::7626:acff:fe5a:b368 [TENTATIVE]
  Global unicast address(es):
    fd82:124::82:124:22:9, subnet is fd82:124::/64 [TENTATIVE]
  Joined group address(es):
    ff02::1:ff22:9
    ff02::6
    ff02::2
    ff02::5
    ff02::1
    ff02::1:ff5a:b368
83net is down, line protocol is down
  IPv6 is enabled, link-local address is fe80::7626:acff:fe5a:b368 [TENTATIVE]
  Global unicast address(es):
    fd83:124::83:124:22:9, subnet is fd83:124::/64 [TENTATIVE]
  Joined group address(es):
    ff02::1:ff22:9
    ff02::2
    ff02::1
    ff02::1:ff5a:b368
nlp_int_tap is up, line protocol is up
  IPv6 is enabled, link-local address is fe80::200:1ff:fe00:1
  Global unicast address(es):
    fd00:0:0:1::1, subnet is fd00:0:0:1::/64
  Joined group address(es):
    ff02::1:ff00:1
    ff02::1
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 1000 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.

------------------ show fragment ------------------
```

```
Interface: outside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: management
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0


------------------ show nve ------------------

------------------ show flow-offload info detail ------------------

Current running state        : Enabled
User configured state        : Enabled
Offload App                  : Running
Offload allocated cores      : S0[ 1] S1[ 18]
Offload reserved Nic         : 9 22
Max PKT burst                : 32
Port-0 details :
        RX queue number      :            277
        FQ queue number      :           1813
        Keep alive counter   :           4854
Port-1 details :
        RX queue number      :            275
        FQ queue number      :           1811
        Keep alive counter   :           4854

------------------ show flow-offload statistics ------------------

Packet stats of port : 0
        Tx Packet count                 :               0
        Rx Packet count                 :               0
        Dropped Packet count            :               0
        VNIC transmitted packet         :               0
        VNIC transmitted bytes          :               0
        VNIC Dropped packets            :               0
        VNIC erroneous received         :               0
        VNIC CRC errors                 :               0
        VNIC transmit failed            :               0
        VNIC multicast received         :               0
 Packet stats of port : 1
        Tx Packet count                 :               0
        Rx Packet count                 :               0
        Dropped Packet count            :               0
        VNIC transmitted packet         :               0
        VNIC transmitted bytes          :               0
        VNIC Dropped packets            :               0
        VNIC erroneous received         :               0
        VNIC CRC errors                 :               0
        VNIC transmit failed            :               0
        VNIC multicast received         :               0

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show asp table socket ------------------
```

```
Protocol    Socket    State      Local Address        Foreign Address
SSL         00002c68  LISTEN     10.86.193.26:443     0.0.0.0:*
TCP         00005a18  LISTEN     10.86.193.26:22      0.0.0.0:*
```

関連コマンド

コマンド	説明
show clock	Syslog サーバ（PFSS）および公開キー インフラストラクチャ（PKI）プロトコルで使用されるクロックを表示します。
show conn count	使用されている接続と使用可能な接続を表示します。
show cpu	CPU の使用状況に関する情報を表示します。
show failover	接続のステータスおよびアクティブになっている ASA を表示します。
show memory	物理メモリの最大量およびオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。
show perfmon	ASA のパフォーマンスに関する情報を表示します。
show processes	動作しているプロセスのリストを表示します。
show running-config	ASA 上で現在実行されているコンフィギュレーションを表示します。
show xlate	変換スロットに関する情報を表示します。

show telemetry

テレメトリデータを表示するには、特権 EXEC モードで **show telemetry** コマンドを使用します。データが JSON 形式で表示されます。

show telemetry [history | last-report | sample]

構文の説明

history	(オプション)テレメトリの設定とアクティビティに関連する過去 100 のイベントを表示します。
last-report	(オプション)FXOS に送信された最新のテレメトリデータを JSON 形式で表示します。
sample	(オプション)即時に生成されたテレメトリデータを JSON 形式で表示します。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォールモード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

service telemetry コマンドはデフォルトで有効になっています。最後に送信したテレメトリデータを表示するか、テレメトリの設定とアクティビティに関連する最新の 100 イベントを表示するかを選択できます。

例

次に、**show telemetry** コマンドの出力例を示します。

```
ciscoasa# show telemetry history

Jan 9 2019 1:00:03:  Telemetry request from FXOS received. SSE connector status:
connected. Telemetry config on Lina: disabled. Telemetry data Not Sent.
Jan 10 2019 0:10:11: Telemetry support on FXOS: disabled
Jan 11 2019 0:15:17: Telemetry support on FXOS: enabled
Jan 11 2019 1:00:02:  Telemetry request from FXOS received. SSE connector status:
connected. Telemetry config on Lina: disabled. Telemetry data Not Sent.
```

```
Jan 11 2019 2:02:02 Telemetry config on Lina: enabled
Jan 12 2019 1:00:02:  Telemetry request  from FXOS received. SSE connector status:
connected. Telemetry config on Lina: enabled. Telemetry data Sent.
```

関連コマンド

コマンド	説明
no service telemetry	テレメトリサービスを無効にします。
show running-config	設定されているデフォルト以外のテレメトリ設定のみを表示します。
show running-config all	設定済みのテレメトリ設定を表示します。

show terminal

現在の CLI セッションの端末設定を表示するには、特権 EXEC モードで **show terminal** コマンドを使用します。

show terminal

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	コマンドが追加されました。

使用上のガイドライン

次のコマンドを使用して端末のプロパティを設定します。

- **terminal interactive**：CLI で **?** を入力すると、現在の CLI セッションでヘルプを有効にします。
- **terminal monitor**：現在の CLI セッションで syslog メッセージが表示されるようにします。
- **terminal width**：コンソール セッション中に表示する情報の幅を設定します。

show terminal コマンドでは **terminal pager** の設定は表示されません。

例

次に、**show terminal** コマンドの出力例を示します。

```
ciscoasa# show terminal

Width = 80, no monitor
terminal interactive
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal interactive	CLI で **?** を入力すると、現在の CLI セッションでヘルプを有効にします。
terminal monitor	現在の CLI セッションで syslog メッセージが表示されるようにします。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	コンソール セッション中に表示する情報の幅を設定します。

show threat-detection memory

threat-detection statistics コマンドによりイネーブルにされる、脅威検出の詳細統計情報で使用されるメモリを表示するには、特権 EXEC モードで **show threat-detection memory** コマンドを使用します。

show threat-detection memory

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

統計情報によっては、大量のメモリを使用して、ASA のパフォーマンスに影響を与えることがあります。このコマンドを使用すると、必要に応じてコンフィギュレーションを調整できるようにメモリ使用率をモニタできます。

例

次に、**show threat-detection memory** コマンドの出力例を示します。

```
ciscoasa# show threat-detection memory
Cached chunks:
       CACHE TYPE              BYTES USED
TD Host                          70245888
TD Port                              2724
TD Protocol                          1476
TD ACE                                728
TD Shared counters                  14256
============================
Subtotal TD Chunks               70265072
```

```
Regular memory                BYTES USED
TD Port                            33824
TD Control block                  162064
============================
Subtotal Regular Memory           195888


Total TD memory:                70460960
```

関連コマンド

コマンド	説明
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection statistics	脅威検出の詳細統計情報をイネーブルにします。

show threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにすると、特権 EXEC モードで **show threat-detection rate** コマンドを使用して統計情報を表示できます。

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

構文の説明

acl-drop	(任意)アクセス リストで拒否されたためにドロップされたパケットのレートを表示します。
min-display-rate *min_display_rate*	(任意)最小表示レート(毎秒あたりのイベント数)を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
bad-packet-drop	(任意)パケット形式に誤りがあって(invalid-ip-header または invalid-tcp-hdr-length など)拒否されたためにドロップされたパケットのレートを表示します。
conn-limit-drop	(任意)接続制限(システム全体のリソース制限および設定された制限の両方)を超えたためにドロップされたパケットのレートを表示します。
dos-drop	(任意)DoS 攻撃(無効な SPI やステートフル ファイアウォール チェック不合格など)を検出したためにドロップされたパケットのレートを表示します。
fw-drop	(任意)基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレートを表示します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。**interface-drop**、**inspect-drop**、**scanning-threat** など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	(任意)疑わしい ICMP パケットが検出されたためにドロップされたパケットのレートを表示します。
inspect-drop	(任意)アプリケーション インスペクションに不合格だったパケットが原因でドロップされたパケットのレート制限を表示します。
interface-drop	(任意)インターフェイスの過負荷が原因でドロップされたパケットのレート制限を表示します。
scanning-threat	(任意)スキャン攻撃が検出されたためにドロップされたパケットのレートを表示します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。完全スキャン脅威検出(**threat-detection scanning-threat** コマンドを参照)では、このスキャン攻撃レートの情報を取得し、その情報をもとにして、たとえばホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。
syn-attack	(オプション)TCP SYN 攻撃や戻りデータなしの UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレートを表示します。

デフォルト

イベント タイプを指定しない場合、すべてのイベントが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 一定時間における平均レート（イベント/秒）。
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートが制限を超えた回数。
- 固定された期間におけるイベントの合計数

ASA は、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASA は、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 10 分の場合、バースト間隔は 10 秒です。最後のバースト間隔が 3:00:00 から 3:00:10 までであった場合に **show** コマンドを 3:00:15 に使用すると、最後の 5 秒分の情報は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection rate** コマンドの出力例を示します。

```
ciscoasa# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
```

```
10-min DoS attck:                0          0          0                  6
1-hour DoS attck:                0          0          0                 42
10-min Interface:                0          0          0                204
1-hour Interface:               88          0          0             318225
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection scanning-threat

threat-detection scanning-threat コマンドを使用してスキャンによる脅威の検出をイネーブルにした場合は、特権 EXEC モードで **show threat-detection scanning-threat** コマンドを使用すると、攻撃者および攻撃対象と分類されたホストが表示されます。

show threat-detection scanning-threat [**attacker** | **target**]

構文の説明

attacker	（任意）攻撃元ホストの IP アドレスを表示します。
target	（オプション）攻撃対象ホストの IP アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)	見出しテキストに「& Subnet List」を表示するように変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。
9.0	インターフェイス情報が出力に追加されました。

例

次に、**show threat-detection scanning-threat** コマンドの出力例を示します。

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

関連コマンド

コマンド	説明
clear threat-detection shun	排除対象からホストを除外します。
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection shun

threat-detection scanning-threat コマンドを使用してスキャンによる脅威の検出をイネーブルにし、攻撃元ホストを自動的に回避した場合は、特権 EXEC モードで **show threat-detection shun** コマンドを使用すると、現在回避されているホストが表示されます。

show threat-detection shun

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。
9.0	インターフェイス情報が出力に追加されました。

使用上のガイドライン

排除対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

例

次に、**show threat-detection shun** コマンドの出力例を示します。

```
ciscoasa# show threat-detection shun
Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

関連コマンド

コマンド	説明
clear threat-detection shun	排除対象からホストを除外します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection statistics host

threat-detection statistics host コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics host** コマンドを使用するとホスト統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]

構文の説明

ip_address	（任意）特定のホストの統計情報を表示します。
mask	（任意）ホスト IP アドレスのサブネット マスクを設定します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

ASA は、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASA は、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics host** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:             2938               0       0             10580308
  8-hour Sent byte:              367               0       0             10580308
 24-hour Sent byte:              122               0       0             10580308
  1-hour Sent pkts:               28               0       0               104043
  8-hour Sent pkts:                3               0       0               104043
 24-hour Sent pkts:                1               0       0               104043
  20-min Sent drop:                9               0       1                10851
  1-hour Sent drop:                3               0       1                10851
  1-hour Recv byte:             2697               0       0              9712670
  8-hour Recv byte:              337               0       0              9712670
 24-hour Recv byte:              112               0       0              9712670
  1-hour Recv pkts:               29               0       0               104846
  8-hour Recv pkts:                3               0       0               104846
 24-hour Recv pkts:                1               0       0               104846
  20-min Recv drop:               42               0       3                50567
  1-hour Recv drop:               14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                0               0       0                  614
  8-hour Sent byte:                0               0       0                  614
 24-hour Sent byte:                0               0       0                  614
  1-hour Sent pkts:                0               0       0                    6
  8-hour Sent pkts:                0               0       0                    6
 24-hour Sent pkts:                0               0       0                    6
  20-min Sent drop:                0               0       0                    4
  1-hour Sent drop:                0               0       0                    4
  1-hour Recv byte:                0               0       0                  706
  8-hour Recv byte:                0               0       0                  706
 24-hour Recv byte:                0               0       0                  706
  1-hour Recv pkts:                0               0       0                    7
```

表 13-2 に、各フィールドの説明を示します。

表 13-2　show threat-detection statistics host のフィールド

フィールド	説明
ホスト	ホストの IP アドレスを表示します。
tot-ses	ホストがデータベースに追加されて以降の、このホストでの合計セッション数を表示します。

表 13-2　show threat-detection statistics host のフィールド(続き)

フィールド	説明
act-ses	ホストが現在関係しているアクティブなセッションの合計数を表示します。
fw-drop	ファイアウォールでのドロップ数を表示します。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケット ドロップを含む組み合わせレートです。これには、アクセス リストでの拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、および戻りデータなしの UDP セッション攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
insp-drop	アプリケーション インスペクションに不合格になったためにドロップされたパケット数を表示します。
null-ses	ヌル セッションの数を表示します。ヌル セッションとは、タイムアウトするまでの 30 秒以内に完了しなかった TCP SYN セッションと、セッションが開始されてから 3 秒以内にサーバからデータの送信がなかった UDP セッションです。
bad-acc	閉じられた状態のホストのポートに対する不正なアクセスの試行回数を表示します。ポートがヌル セッション状態(上記を参照)であると判定されると、ホストのポート状態は HOST_PORT_CLOSE に設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。
Average(eps)	各間隔における平均レート(イベント数/秒)を表示します。 セキュリティ アプライアンスは、合計 30 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔(1/30 個目)のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在バースト レート(イベント数/秒)を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。

表 13-2　show threat-detection statistics host のフィールド(続き)

フィールド	説明
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔(1/30 個目)のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
20-min、1-hour、8-hour、および 24-hour	デフォルトでは、3 つのレート間隔が表示されます。**threat-detection statistics host number-of-rate** コマンドを使用すると、レート間隔の数を減らすことができます。ホスト統計情報では大量のメモリが使用されるため、レート間隔の数値をデフォルトの 3 より減らすと、メモリ使用率が軽減します。このキーワードを 1 に設定すると、最短のレート間隔統計情報だけが保持されます。値を 2 に設定すると、2 つの最短の間隔が保持されます。
Sent byte	ホストから正常に送信されたバイト数を表示します。
Sent pkts	ホストから正常に送信されたパケット数を表示します。
Sent drop	ホストから送信されたパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数を表示します。
Recv byte	ホストが正常に受信したバイト数を表示します。
Recv pkts	ホストが正常に受信したパケット数を表示します。
Recv drop	ホストが受信したパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics port

threat-detection statistics port コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics port** コマンドを使用すると、TCP ポートおよび UDP ポートの統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[**-***end_port*]]

構文の説明

start_port[**-***end_port*]	（任意）0 ～ 65535 の間の特定のポートまたはポート範囲の統計情報を表示します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

ASA は、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASA は、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics port** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics port

                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939               0       0             10580922
  8-hour Sent byte:                367           22043       0             10580922
 24-hour Sent byte:                122            7347       0             10580922
  1-hour Sent pkts:                 28               0       0               104049
  8-hour Sent pkts:                  3             216       0               104049
 24-hour Sent pkts:                  1              72       0               104049
  20-min Sent drop:                  9               0       2                10855
  1-hour Sent drop:                  3               0       2                10855
  1-hour Recv byte:               2698               0       0              9713376
  8-hour Recv byte:                337           20236       0              9713376
 24-hour Recv byte:                112            6745       0              9713376
  1-hour Recv pkts:                 29               0       0               104853
  8-hour Recv pkts:                  3             218       0               104853
 24-hour Recv pkts:                  1              72       0               104853
  20-min Recv drop:                 24               0       2                29134
  1-hour Recv drop:                  8               0       2                29134
```

表 13-3 に、各フィールドの説明を示します。

表 13-3　show threat-detection statistics port のフィールド

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 30 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

表 13-3　show threat-detection statistics port のフィールド(続き)

フィールド	説明
Current(eps)	終了した最後のバースト間隔における現在バースト レート(イベント数/秒)を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔(1/30 個目)のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
port_number/*port_name*	パケットまたはバイトが送信、受信、またはドロップされた、ポートの番号と名前を表示します。
tot-ses	このポートのセッションの合計数を表示します。
act-ses	ポートが現在関係しているアクティブなセッションの合計数を表示します。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	ポートから正常に送信されたバイト数を表示します。
Sent pkts	ポートから正常に送信されたパケット数を表示します。
Sent drop	スキャン攻撃の一部であったためにドロップされた、ポートから送信されたパケット数を表示します。
Recv byte	ポートが正常に受信したバイト数を表示します。
Recv pkts	ポートが正常に受信したパケット数を表示します。
Recv drop	スキャン攻撃の一部であったためにドロップされた、ポートが受信したパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics protocol

threat-detection statistics protocol コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics protocol** コマンドを使用すると、IP プロトコルの統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol_name*]

構文の説明

protocol_number	(任意)0 ～ 255 の間の特定のプロトコル番号の統計情報を表示します。
min-display-rate *min_display_rate*	(任意)最小表示レート(毎秒あたりのイベント数)を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
protocol_name	(任意)特定のプロトコル名の統計情報を表示します。 • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

ASA は、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASA は、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics protocol** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics protocol

                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0               0       0                 1000
  8-hour Sent byte:                  0               2       0                 1000
 24-hour Sent byte:                  0               0       0                 1000
  1-hour Sent pkts:                  0               0       0                   10
  8-hour Sent pkts:                  0               0       0                   10
 24-hour Sent pkts:                  0               0       0                   10
```

表 13-4 に、各フィールドの説明を示します。

表 13-4　show threat-detection statistics protocol のフィールド

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 30 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
protocol_number/ *protocol_name*	パケットまたはバイトが送信、受信、またはドロップされた、プロトコルの番号と名前を表示します。
tot-ses	現在使用されていません。
act-ses	現在使用されていません。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	プロトコルから正常に送信されたバイト数を表示します。
Sent pkts	プロトコルから正常に送信されたパケット数を表示します。
Sent drop	スキャン攻撃の一部であったためにドロップされた、プロトコルから送信されたパケット数を表示します。
Recv byte	プロトコルが正常に受信したバイト数を表示します。

表 13-4　show threat-detection statistics protocol のフィールド(続き)

フィールド	説明
Recv pkts	プロトコルが正常に受信したパケット数を表示します。
Recv drop	スキャン攻撃の一部であったためにドロップされた、プロトコルが受信したパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics top

threat-detection statistics コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics top** コマンドを使用すると、上位 10 件の統計情報が表示されます。特定のタイプで脅威の検出の統計情報がイネーブルでない場合、このコマンドではそれらの統計情報を表示できません。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] [**detail**] [**long**]]

構文の説明

access-list	(任意)許可 ACE と拒否 ACE の両方を含む、パケットに一致する上位 10 件の ACE を表示します。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにすると、**show threat-detection rate access-list** コマンドを使用してアクセス リストの拒否を追跡できます。
all	(任意)TCP 代行受信の場合、追跡されたすべてのサーバの履歴データを表示します。
detail	(任意)TCP 代行受信の場合、サンプリング データの履歴を表示します。
ホスト	(任意)一定期間ごとに上位 10 件のホスト統計情報を表示します。 (注) 脅威の検出アルゴリズムにより、フェールオーバー リンクまたはステート リンクに使用するインターフェイスは、上位 10 のホストの 1 つとして表示される可能性があります。この現象は、フェールオーバー リンクとステート リンクの両方に 1 つのインターフェイスを使用するときに発生する可能性が高くなります。これは正常な動作であり、この IP アドレスが表示されても無視してかまいません。
long	(任意)サーバの実際の IP アドレスおよび無変換の IP アドレスとともに、統計情報の履歴をロング フォーマットで表示します。
min-display-rate *min_display_rate*	(任意)最小表示レート(毎秒あたりのイベント数)を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
port-protocol	(任意)TCP/UDP ポート タイプと IP プロトコル タイプを組み合わせた上位 10 件の統計情報を表示します。TCP(プロトコル 6)と UDP(プロトコル 17)は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ(ポートまたはプロトコル)の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。
rate-1	(任意)表示されている一定レート間隔のうち、最小のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-1** キーワードを使用すると、1 時間間隔だけが ASA に表示されます。
rate-2	(任意)表示されている一定レート間隔のうち、中間のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-2** キーワードを使用すると、8 時間間隔だけが ASA に表示されます。

rate-3	(任意)表示されている一定レート間隔のうち、最大のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-3** キーワードを使用すると、24 時間間隔だけが ASA に表示されます。
tcp-intercept	TCP 代行受信の統計情報を表示します。表示には、攻撃を受けて保護された上位 10 サーバが含まれます。

デフォルト

イベント タイプを指定しない場合、すべてのイベントが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)	**tcp-intercept** キーワードが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	**tcp-intercept** に **long** キーワードが追加されました。脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート(イベント数/秒)
- 終了した最後のバースト間隔における現在のバースト レート(イベント数/秒)。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数(ドロップされたトラフィックの統計情報の場合に限る)
- 固定された期間におけるイベントの合計数

ASA は、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASA は、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics top access-list** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics top access-list

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]              173                0       0                623488
              200/2[1]               43                0       0                156786
              100/1[2]               43                0       0                156786
  8-hour ACL hits:
              100/3[0]               21             1298       0                623488
              200/2[1]                5              326       0                156786
              100/1[2]                5              326       0                156786
```

表 13-5 に、各フィールドの説明を示します。

表 13-5　show threat-detection statistics top access-list のフィールド

フィールド	説明
上	[0]（最高数）から [9]（最低数）の範囲で、時間内の ACE のランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示される ACE が 10 件未満となります。
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 30 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明の例では、現在のレートは 3:19:30 から 3:20:00 となります。
Trigger	アクセス リスト トラフィックがトリガーするレート制限は設定されていないため、この列は常に 0 です。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにすると、**show threat-detection rate access-list** コマンドを使用してアクセス リストの拒否を追跡できます。

表 13-5　show threat-detection statistics top access-list のフィールド(続き)

フィールド	説明
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔(1/30 個目)のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
1-hour、8-hour	これらの固定レート間隔における統計情報を表示します。
acl_name/line_number	拒否される原因となった ACE のアクセス リスト名および行番号を表示します。

次に、**show threat-detection statistics top access-list rate-1** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics top access-list rate-1

                    Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]             173               0       0               623488
              200/2[1]              43               0       0               156786
              100/1[2]              43               0       0               156786
```

次に、**show threat-detection statistics top port-protocol** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics top port-protocol

Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher   70              71               0       0          32345678
 2  btp-clnt/dhcp   68              68               0       0          27345678
 3         gopher   69              65               0       0          24345678
 4    Protocol-96 * 96              63               0       0          22345678
 5      Port-7314 7314              62               0       0          12845678
 6 BitTorrent/trc 6969              61               0       0          12645678
 7     Port-8191-65535              55               0       0          12345678
 8           SMTP  366              34               0       0           3345678
 9         IPinIP *  4              30               0       0           2345678
10          EIGRP * 88              23               0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

表 13-6 に、各フィールドの説明を示します。

表 13-6　show threat-detection statistics top port-protocol のフィールド

フィールド	説明
上	[0]（最高数）から [9]（最低数）の範囲で、統計情報の時間内かタイプにあるポートまたはプロトコルのランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示されるポート/プロトコルが 10 件未満となります。
名前	ポートまたはプロトコル名を表示します。
Id	ポート ID 番号またはプロトコル ID 番号を表示します。アスタリスク (*) は、その ID が IP プロトコル番号であることを意味します。
Average(eps)	表 13-2 の説明を参照してください。
Current(eps)	表 13-2 の説明を参照してください。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	表 13-2 の説明を参照してください。
Time_interval Sent byte	各期間において、表示されたポートおよびプロトコルから正常に送信されたバイト数を表示します。
Time_interval Sent packet	各期間において、表示されたポートおよびプロトコルから正常に送信されたパケット数を表示します。
Time_interval Sent drop	各期間において、スキャン攻撃の一部であったためにドロップされた、表示されたポートおよびプロトコルから送信されたパケット数を表示します。
Time_interval Recv byte	各期間において、表示されたポートおよびプロトコルで正常に受信したバイト数を表示します。
Time_interval Recv packet	一覧にあるポートおよびプロトコルが正常に受信したパケット数を、時間間隔ごとに表示します。
Time_interval Recv drop	一覧にあるポートおよびプロトコルが受信し、スキャン攻撃の一部であるためにドロップされたパケット数を、時間間隔ごとに表示します。
port_number/ *port_name*	パケットまたはバイトが送信、受信、またはドロップされた、ポートの番号と名前を表示します。
protocol_number/ *protocol_name*	パケットまたはバイトが送信、受信、またはドロップされた、プロトコルの番号と名前を表示します。

次に、**show threat-detection statistics top host** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics top host

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]             2938                0       0              10580308
  1-hour Sent pkts:
          10.0.0.1[0]               28                0       0                104043
  20-min Sent drop:
          10.0.0.1[0]                9                0       1                 10851
```

```
1-hour Recv byte:
        10.0.0.1[0]            2697              0       0              9712670
1-hour Recv pkts:
        10.0.0.1[0]              29              0       0               104846
20-min Recv drop:
        10.0.0.1[0]              42              0       3                50567
8-hour Sent byte:
        10.0.0.1[0]             367              0       0             10580308
8-hour Sent pkts:
        10.0.0.1[0]               3              0       0               104043
1-hour Sent drop:
        10.0.0.1[0]               3              0       1                10851
8-hour Recv byte:
        10.0.0.1[0]             337              0       0              9712670
8-hour Recv pkts:
        10.0.0.1[0]               3              0       0               104846
1-hour Recv drop:
        10.0.0.1[0]              14              0       1                50567
24-hour Sent byte:
        10.0.0.1[0]             122              0       0             10580308
24-hour Sent pkts:
        10.0.0.1[0]               1              0       0               104043
24-hour Recv byte:
        10.0.0.1[0]             112              0       0              9712670
24-hour Recv pkts:
        10.0.0.1[0]               1              0       0               104846
```

表 13-7 に、各フィールドの説明を示します。

表 13-7　show threat-detection statistics top host のフィールド

フィールド	説明
上	[0]（最高数）から [9]（最低数）の範囲で、統計情報の時間内かタイプにあるホストのランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示されるホストが 10 件未満となります。
Average(eps)	表 13-2 の説明を参照してください。
Current(eps)	表 13-2 の説明を参照してください。
Trigger	表 13-2 の説明を参照してください。
Total events	表 13-2 の説明を参照してください。
Time_interval Sent byte	各期間において、表示されたホストに正常に送信されたバイト数を表示します。
Time_interval Sent packet	各期間において、表示されたホストに正常に送信されたパケット数を表示します。
Time_interval Sent drop	各期間において、スキャン攻撃の一部であったためにドロップされた、表示されたホストに送信されたパケット数を表示します。
Time_interval Recv byte	各期間において、表示されたホストで正常に受信したバイト数を表示します。
Time_interval Recv packet	一覧にあるポートおよびプロトコルが正常に受信したパケット数を、時間間隔ごとに表示します。
Time_interval Recv drop	一覧にあるポートおよびプロトコルが受信し、スキャン攻撃の一部であるためにドロップされたパケット数を、時間間隔ごとに表示します。
host_ip_address	パケットまたはバイトが送信、受信、ドロップされたホスト IP アドレスを表示します。

次に、**show threat-detection statistics top tcp-intercept** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
----------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2     192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3     192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4     192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5     192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6     192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7     192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8     192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9     192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10    192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

表 13-8 に、各フィールドの説明を示します。

表 13-8　show threat-detection statistics top tcp-intercept のフィールド

フィールド	説明
Monitoring window size:	統計情報のために ASA がデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定を変更するには、**threat-detection statistics tcp-intercept rate-interval** コマンドを使用します。ASA は、この間隔でデータを 30 回サンプリングします。
Sampling interval:	サンプリング間の間隔を表示します。この値は、常にレート間隔を 30 で割った数値になります。
rank	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバで、10 位は最も攻撃が少なかったサーバです。
server_ip:port	攻撃を受けているサーバの IP アドレスおよびポートを表示します。
interface	サーバが攻撃を受けているインターフェイスを表示します。
avg_rate	サンプリング期間中の平均攻撃レートを 1 秒あたりの攻撃数で表示します。
current_rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
total	攻撃の合計数を表示します。
attacker_ip	攻撃者の IP アドレスを表示します。
(*last_attack_time* ago)	最後の攻撃が発生した時間を表示します。

次に、**show threat-detection statistics top tcp-intercept long** コマンドの出力例を示します。実際の送信元 IP アドレスがカッコ内に表示されています。

```
ciscoasa# show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total>
<Source IP (Last Attack Time)>
----------------------------------------------------------------------------------
1     10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2     10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3     10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

```
4     10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5     10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6     10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7     10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8     10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9     10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10    10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

次に、**show threat-detection statistics top tcp-intercept detail** コマンドの出力例を示します。

```
ciscoasa# show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
      Sampling History (30 Samplings):
              95348      95337      95341      95339      95338      95342
              95337      95348      95342      95338      95339      95340
              95339      95337      95342      95348      95338      95342
              95337      95339      95340      95339      95347      95343
              95337      95338      95342      95338      95337      95342
              95348      95338      95342      95338      95337      95343
              95337      95349      95341      95338      95337      95342
              95338      95339      95338      95350      95339      95570
              96351      96351      96119      95337      95349      95341
              95338      95337      95342      95338      95338      95342
......
```

表 13-9 に、各フィールドの説明を示します。

表 13-9　show threat-detection statistics top tcp-intercept detail のフィールド

フィールド	説明
Monitoring window size:	統計情報のために ASA がデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定を変更するには、**threat-detection statistics tcp-intercept rate-interval** コマンドを使用します。ASA は、この間隔でデータを 30 回サンプリングします。
Sampling interval:	サンプリング間の間隔を表示します。この値は、常にレート間隔を 30 で割った数値になります。
rank	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバで、10 位は最も攻撃が少なかったサーバです。
server_ip:port	攻撃を受けているサーバの IP アドレスおよびポートを表示します。
interface	サーバが攻撃を受けているインターフェイスを表示します。
avg_rate	**threat-detection statistics tcp-intercept rate-interval** コマンドで設定されたレート間隔での平均攻撃レートを、1 秒あたりの攻撃数で表示します（デフォルトのレート間隔は 30 分です）。レート間隔中、ASA は 30 秒ごとにデータをサンプリングします。
current_rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
total	攻撃の合計数を表示します。
attacker_ip or <*various*> Last: *attacker_ip*	攻撃者の IP アドレスを表示します。複数の攻撃者がいる場合は、「<various>」の後に最後の攻撃者の IP アドレスが表示されます。

表 13-9　show threat-detection statistics top tcp-intercept detail のフィールド(続き)

フィールド	説明
(*last_attack_time* ago)	最後の攻撃が発生した時間を表示します。
sampling data	30 個のサンプリング データ値をすべて表示します。間隔ごとの攻撃回数が表示されます。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show time-range

すべての時間範囲オブジェクトの設定を表示するには、特権 EXEC モードで**show time-range** コマンドを使用します。

show time-range [*name*]

構文の説明

name	（オプション）この時間範囲オブジェクトの情報のみを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、時間範囲オブジェクトの設定を表示する例を示します。この例では、work-hours という名前のオブジェクトが 1 つあります。inactive は、オブジェクトが使用されていないことを意味します。

```
ciscoasa# show time-range

time-range entry: work-hours (inactive)
   periodic weekdays 9:00 to 17:00
```

関連コマンド

コマンド	説明
time-range	時間範囲オブジェクトを設定します。

show tls-proxy

TLS プロキシおよびセッション情報を表示するには、グローバル コンフィギュレーション モードで **show tls-proxy** コマンドを使用します。

show tls-proxy [*tls_name* **| [session [host** *host_addr* **| detail [cert-dump] | count | statistics]]]**

構文の説明

cert-dump	ローカル ダイナミック証明書をダンプします。出力は LDC の 16 進ダンプです。
count	セッション カウンタだけを表示します。
detail[cert-dump]	各 SSL レッグおよび LDC の暗号を含む詳細な TLS プロキシ情報を表示します。**cert dump** キーワードを追加して、ローカルダイナミック証明書（LDC）の 16 進数のダンプを取得します。 これらのキーワードを **host** オプションとともに使用することもできます。
host *host_addr*	関連付けられたセッションを表示する特定のホストの IPv4 または IPv6 アドレスを指定します。
session	アクティブな TLS プロキシ セッションを表示します。
statistics	TLS セッションをモニタおよび管理するための統計情報を表示します。
tls_name	表示する TLS プロキシの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.3(1)	**statistics** キーワードが追加されました。

例

次に、**show tls-proxy** コマンドの出力例を示します。

```
ciscoasa# show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
    Server proxy:
        Trust-point: local_ccm
```

```
    Client proxy:
        Local dynamic certificate issuer: ldc_signer
        Local dynamic certificate key-pair: phone_common
        Cipher-suite <unconfigured>
    Run-time proxies:
        Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
            Active sess 1, most sess 4, byte 3244
```

次に、**show tls-proxy session** コマンドの出力例を示します。

```
ciscoasa# show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

次に、**show tls-proxy session detail** コマンドの出力例を示します。

```
ciscoasa# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
    Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
    Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
    Status: Available
    Certificate Serial Number: 29
    Certificate Usage: General Purpose
    Public Key Type: RSA (1024 bits)
    Issuer Name:
        cn=TLS-Proxy-Signer
    Subject Name:
        cn=SEP0002B9EB0AAD
        o=Cisco Systems Inc
        c=US
    Validity Date:
        start date: 00:47:12 PDT Feb 27 2007
        end   date: 00:47:12 PDT Feb 27 2008
    Associated Trustpoints:
```

次に、**show tls-proxy session statistics** コマンドの出力例を示します。

```
ciscoasa# show tls-proxy session stastics
TLS Proxy Sessions (Established: 600)
    Mobility:                                       0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
    SIP:                                            2
    SCCP:                                          20
    DIAMETER:                                     200
Total TLS Proxy Sessions
    Established:                                  822
    Platform Limit:                              1000
```

関連コマンド

コマンド	説明
クライアント	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキー ペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。

コマンド	説明
show running-config tls-proxy	すべてまたは指定された TLS プロキシの実行コンフィギュレーションを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

show track

セキュリティレベル合意(SLA)トラッキング プロセスが追跡したオブジェクトに関する情報を表示するには、ユーザ EXEC モードで **show track** コマンドを使用します。

show track [*track-id*]

構文の説明

track-id	トラッキング エントリ オブジェクト ID 番号(1 ~ 500)。

デフォルト

track-id が指定されなかった場合は、すべてのトラッキング オブジェクトに関する情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、**show track** コマンドの出力例を示します。

```
ciscoasa(config)# show track

Track 5
    Response Time Reporter 124 reachability
    Reachability is UP
    2 changes, last change 03:41:16
    Latest operation return code: OK
    Tracked by:
        STATIC-IP-ROUTING 0
```

関連コマンド

コマンド	説明
show running-config track	実行コンフィギュレーションの **track rtr** コマンドを表示します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

show traffic

インターフェイスの送信アクティビティと受信アクティビティを表示するには、特権 EXEC モードで **show traffic** コマンドを使用します。

show traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	ASA 5550 の出力が追加されました。
9.3(1)	物理インターフェイスの集約トラフィックの出力が追加されました。
9.5(2)	SCTP および SCTP インスペクションが詳細な出力に追加されました。

使用上のガイドライン

show traffic コマンドは、**show traffic** コマンドが最後に入力された時点または ASA がオンラインになった時点以降に、各インターフェイスを通過したパケットの数とバイト数を表示します。秒数は、ASA が直前のリブート以降、オンラインになってからの経過時間です（直前のリブート以降に **clear traffic** コマンドが入力されていない場合）。コマンドが入力されていた場合は、コマンドが入力された時点からの経過時間となります。

ASA 5550 の場合、**show traffic** コマンドを実行するとスロットごとの集約スループットも表示されます。ASA 5550 のスループットを最大にするには、トラフィックをスロットに均一に分散する必要があります。この出力は、トラフィックが均一に分散しているかどうかを確認するのに役立ちます。

物理インターフェイスの集約トラフィックを表示するには、最初に **sysopt traffic detailed-statistics** コマンドを入力して、この機能をオンにする必要があります。

例

次に、**show traffic** コマンドの出力例を示します。

```
ciscoasa# show traffic
outside:
        received (in 102.080 secs):
                2048 packets 204295 bytes
                20 pkts/sec 2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 204056 bytes
                20 pkts/sec 1998 bytes/sec

Ethernet0:
        received (in 102.080 secs):
                2049 packets 233027 bytes
                20 pkts/sec 2282 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 232750 bytes
                20 pkts/sec 2280 bytes/sec
```

ASA 5550 の場合、次のテキストが最後に表示されます。

```
---------------------------------------
        Per Slot Throughput Profile
---------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|****************
    Slot 1:       3149  50%|****************

  Bytes-per-second profile:
    Slot 0:     427044  50%|****************
    Slot 1:     427094  50%|****************
```

次に、物理インターフェイスの集約トラフィック用に追加された出力例を示します。

```
IP packet size distribution (values listed in percentages)
Total Packets = 1278:
      32    64    96   128   192   256   512
    00.0  43.5  10.4  10.1  26.1  01.4  03.6

    1024  1536  2048  4096  8192  9216
    03.6  06.6  00.0  00.0  00.0  00.0

Protocol          Total    Conns   Packets   Bytes  Packets    Total
--------          Conns     /Sec     /Conn    /Pkt     /Sec  Packets
SCTP                  0      0.0         0       0      0.0        0
SCTP-inspected        0      0.0       N/A     N/A      0.0        0
TCP                   8      0.2        98     215     26.8     1279
TCP-inspected         0      0.0       N/A     N/A      0.0        0
UDP                   3      0.0         0      90      0.0        2
UDP-inspected         5      0.0         1     189      0.0       56
ICMP                  0      0.0         1      98      0.0        2
ESP                   0      0.0       N/A     N/A      0.0        0
IP                    0      0.0       N/A     N/A      0.0        0
Total:               16      0.2        22     207     26.8     1433

Last clearing of statistics: Never
```

関連コマンド

コマンド	説明
clear traffic	送信アクティビティと受信アクティビティのカウンタをリセットします。

CHAPTER 14

show uauth through show zone Commandsw

show uauth

現在認証済みの 1 名またはすべてのユーザ、ユーザがバインドされているホスト IP、および キャッシュされた IP とポートの認可情報を表示するには、特権 EXEC モードで **show uauth** コマンドを使用します。

show uauth [*username*]

構文の説明

username	(任意)表示するユーザ認証情報とユーザ認可情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認可情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	アイドル時間が出力に追加されました。
7.2(2)	アイドル時間が出力から削除されました。

使用上のガイドライン

show uauth コマンドは、1 名またはすべてのユーザの AAA 認可キャッシュおよび認証キャッシュを表示します。

このコマンドは、**timeout** コマンドとともに使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。このキャッシュでは、ユーザ ホストごとに 16 個までのアドレスとサービスのペアが許可されます。正しいホストからキャッシュされているサービスにユーザがアクセスしようとした場合、ASA ではそのアクセスが事前に許可されていると見なし、その接続を即座に代理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。この処理により、パフォーマンスが大幅に向上され、認可サーバの負荷が削減されます。

show uauth コマンドの出力には、認証と認可のために認可サーバに渡されたユーザ名、そのユーザ名がバインドされている IP アドレス、およびこのユーザが認証されたのみであるか、または、キャッシュされたサービスがあるかが表示されます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能とともに Xauth を使用すると、ネットワーク間に IPsec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウンティング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、**aaa** コマンドを参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、いずれのユーザも認証されておらず、かつ、1 つのユーザ認証が進行している場合の **show uauth** コマンドの出力例を示します。

```
ciscoasa(config)# show uauth
                        Current    Most Seen
Authenticated Users       1           1
Authen In Progress        0           1
user 'v039294' at 136.131.178.4, authenticated (idle for 0:00:00)
   access-list #ACSACL#-IP-v039294-521b0b8b (*)
   absolute   timeout: 0:00:00
   inactivity timeout: 0:05:00
```

次に、3 人のユーザが認証されており、かつ、ASA を介してサービスを使用することが認可されている場合の **show uauth** コマンドの出力例を示します。

```
ciscoasa(config)# show uauth
user ‘pat’ from 209.165.201.2 authenticated
user ‘robin’ from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user ‘terry’ from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

関連コマンド

コマンド	説明
clear uauth	現在のユーザの認証情報と認可情報を削除します。
timeout	アイドル時間の最大継続期間を設定します。

show url-block

url-block バッファに保持されているパケット数と、バッファ上限を超えたか再送信のためにドロップされたパケット数（ある場合）を表示するには、特権 EXEC モードで **show url-block** コマンドを使用します。

show url-block [**block statistics**]

構文の説明

block statistics	（任意）ブロック バッファの使用状況に関する統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show url-block block statistics コマンドは、URL ブロック バッファに保持されているパケット数と、バッファ上限を超えたか再送信のためにドロップされたパケット数（ある場合）を表示します。

例

次に、**show url-block** コマンドの出力例を示します。

```
ciscoasa# show url-block
|url-block url-mempool 128|url-block url-size 4|url-block block 128
```

URL ブロック バッファのコンフィギュレーションが表示されています。

次に、**show url-block block statistics** コマンドの出力例を示します。

```
ciscoasa# show url-block block statistics

URL Pending Packet Buffer Stats with max block  128|
Cumulative number of packets held:|896
Maximum number of packets held (per URL):|3
Current number of packets held (global):|38
```

```
Packets dropped due to
| exceeding url-block buffer limit: | 7546
| HTTP server retransmission: | 10
Number of packets released back to client: | 0
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファの使用状況カウンタをクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show url-cache statistics

N2H2 または Websense のフィルタリング サーバから受信した URL 応答に使用される URL キャッシュの情報を表示するには、特権 EXEC モードで **show url-cache statistics** コマンドを使用します。

show url-cache statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show url-cache statistics コマンドには、次のエントリが表示されます。

- Size：キャッシュ サイズ（KB 単位）。**url-cache** *size* オプションを使用して設定します。
- Entries：キャッシュ サイズに基づくキャッシュ エントリの最大数。
- In Use：キャッシュに含まれる現在のエントリ数。
- Lookups：ASA がキャッシュ エントリを検索した回数。
- Hits：ASA がキャッシュ内でエントリを検出した回数。

show perfmon コマンドを使用すると、N2H2 Sentian または Websense のフィルタリング アクティビティに関する追加情報を表示できます。

例

次に、**show url-cache statistics** コマンドの出力例を示します。

```
ciscoasa# show url-cache statistics

URL Filter Cache Stats
----------------------
 Size :     1KB
 Entries :     36
  In Use :     30
 Lookups :     300
 Hits :     290
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド ステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバから受信した応答の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show url-server

URL フィルタリング サーバに関する情報を表示するには、特権 EXEC モードで **show url-server** コマンドを使用します。

show url-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show url-server statistics コマンドは、URL サーバのベンダーおよびステータスを表示します。また、URL、HTTPS 接続、および TCP 接続について、合計数、許可された数、拒否された数を表示します。

show url-server コマンドには、次の情報が表示されます。

- N2H2 の場合：**url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol** [{**TCP | UDP**}{**version 1 | 4**}]
- Websense の場合：**url-server (***if_name***) vendor websense host** *local_ip* **timeout** *seconds* **protocol** [{**TCP | UDP**}]

例

次に、**show url-server statistics** コマンドの出力例を示します。

```
ciscoasa## show url-server statistics
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
```

```
FTPs total/allowed/denied          994387/155648/838739
FTPs allowed by cache/server       70483/85165
FTPs denied by cache/server        801920/36819
Requests dropped                   28715
Server timeouts/retries            567/1350
Processed rate average 60s/300s    1524/1344 requests/second
Denied rate average 60s/300s       35648/33022 requests/second
Dropped rate average 60s/300s      156/189 requests/second

URL Server Statistics:
----------------------
192.168.0.1                        UP
Vendor                             websense
Port                               17035
Requests total/allowed/denied      366519/255495/110457
Server timeouts/retries            567/1350
Responses received                 365952
Response time average 60s/300s     2/1 seconds/request
192.168.0.2                        DOWN
Vendor                             websense
Port                               17035
Requests total/allowed/denied      0/0/0
Server timeouts/retries            0/0
Responses received                 0
Response time average 60s/300s     0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message                  Sent    Received
STATUS_REQUEST           411     0
LOOKUP_REQUEST           366519  365952
LOG_REQUEST              0       NA

Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0

Semantics:
This command allows the operator to display url-server statistics organized on a global
and per-server basis. The output is reformatted to provide: more-detailed information and
per-server organization.

Supported Modes:
privileged
router || transparent
single || multi/context

Privilege:
ATTR_ES_CHECK_CONTEXT

Debug support:
N/A

Migration Strategy (if any):
N/A
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報をクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show user-alert

すべてのアクティブなクライアントレス WebVPN セッションに対して表示できる、現在設定されているユーザ アラートを表示するには、特権 EXEC モードで **show user-alert** コマンドを使用します。

show user-alert

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

関連コマンド

コマンド	説明
user-alert	現在のアクティブ セッションのすべてのクライアントレス SSL VPN ユーザに対する緊急メッセージのブロードキャストをイネーブルにします。

show user-identity ad-agent

アイデンティティ ファイアウォールの AD エージェントに関する情報を表示するには、特権 EXEC モードで **show user-identity ad-agent** コマンドを使用します。

show user-identity ad-agent [**statistics**]

構文の説明

statistics	（オプション）AD エージェントに関する統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォールの AD エージェント コンポーネントをモニタできます。

AD エージェントのトラブルシューティング情報を取得するには、**show user-identity ad-agent** コマンドを使用します。このコマンドは、プライマリ AD エージェントおよびセカンダリ AD エージェントに関する次の情報を表示します。

- AD エージェントのステータス
- ドメインのステータス
- AD エージェントの統計情報

表 14-1　コマンド出力の説明

タイプ	値	説明
モード	コンフィギュレーション モード	フル ダウンロードまたはオンデマンド ダウンロードを指定します。
AD Agent IP Address	IP address	アクティブな AD エージェントの IP アドレスを表示します。
バックアップ	IP address	バックアップの AD エージェントの IP アドレスを表示します。

表 14-1　コマンド出力の説明(続き)

タイプ	値	説明
AD Agent Status	• ディセーブル • Down • Up (registered) • Probing	• アイデンティティ ファイアウォールはディセーブルです。 • AD エージェントはダウンしています。 • AD エージェントは稼働しています。 • ASA は登録され、AD エージェントが稼働しています。 • ASA は AD エージェントに接続しようとしています。
Authentication Port	udp/1645	AD エージェントの認証ポートを表示します。
Accounting Port	udp/1646	AD エージェントのアカウンティング ポートを表示します。
ASA Listening Port	udp/3799	ASA リスニング ポートを表示します。
インターフェイス	インターフェイス	AD エージェントと通信するために ASA が使用するインターフェイスを表示します。
IP Address	IP address	AD エージェントと通信するために ASA が使用する IP アドレスを表示します。
Uptime	時刻	AD エージェントのアップ タイムを表示します。
Average RTT	ミリ秒	AD エージェントと通信するために ASA を使用する平均ラウンド トリップ時間を表示します。
ドメイン(Domain)	ドメイン ニックネーム Status: up Status: down	AD エージェントの Microsoft Active Directory ドメインを表示します。

例

次に、アイデンティティ ファイアウォールの AD エージェントの情報を表示する例を示します。

```
ciscoasa# show user-identity ad-agent
Primary AD Agent:
 Status                    up (registered)
 Mode:                     full-download
 IP address:               172.23.62.125
 Authentication port:      udp/1645
 Accounting port:          udp/1646
 ASA Listening port:       udp/3799
 Interface:                mgmt
 Up time:                  15 mins 41 secs
 Average RTT:              57 msec

Secondary AD Agent:
 Status                    up
 Mode:                     full-download
 IP address:               172.23.62.136
 Authentication port:      udp/1645
 Accounting port:          udp/1646
 ASA Listening port:       udp/3799
 Interface:                mgmt
 Up time:                  7 mins 56 secs
 Avg RTT:                  15 msec
```

関連コマンド

コマンド	説明
clear user-identity ad-agent statistics	アイデンティティ ファイアウォールの ASA によって保持されている AD エージェントの統計データをクリアします。
user-identity enable	Cisco Identity Firewall インスタンスを作成します。
show user-identity ad-group-members	アイデンティティ ファイアウォールの AD エージェントのドメインにあるグループ メンバーを表示します。

show user-identity ad-group-members

アイデンティティ ファイアウォールの AD エージェント のドメインにあるグループ メンバーを表示するには、特権 EXEC モードで **show user-identity ad-group-members** コマンドを使用します。

show user-identity ad-group-members [*domain_nickname*\]*user_group_name* [**timeout seconds** *seconds*]

構文の説明

domain_nickname	(オプション)アイデンティティ ファイアウォールのドメイン名を指定します。
timeout seconds *seconds*	(オプション)グループ メンバーの統計情報を取得するタイマーを設定して、タイマーの期間を指定します。
user_group_name	(オプション)統計情報を取得するグループ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

show user-identity ad-group-members コマンドは、指定したユーザ グループの直近メンバー(ユーザとグループ)を表示します。

(注) このコマンドでは、**object-group user** コマンドを使用して設定された、ASA 上のローカルに定義されたグループの情報は表示されません。

ASA は、Active Directory サーバで設定された Active Directory グループに対する LDAP クエリーを送信します。このコマンドを実行することは、指定したユーザ グループのメンバーをチェックできる LDAP ブラウザ コマンドを実行することと同等です。ASA は、1 つのレベルの LDAP クエリーを発行して、distinguishedName 形式で指定したグループの直近メンバーを取得します。このコマンドを実行しても、インポートされたユーザ グループの ASA 内部キャッシュは更新されません。

domain_nickname を指定しない場合、ASA はデフォルト ドメインに *user_group_name* があるグループの情報を表示します。*domain_nickname* 引数には、実際のドメイン ニックネームまたは LOCAL を指定できます。

グループ名は、CN 名ではなく AD グループの一意の sAMAccountName になります。特定グループの sAMAccountName の情報を表示するには、**show user-identity ad-groups filter** *filter_string* コマンド を使用して、グループの sAMAccountName を取得します。

例

次に、アイデンティティ ファイアウォールのグループ sample1 のメンバーを表示する例を示します。

```
ciscoasa# show user-identity ad-group-member group.sample1
Domain:CSCO        AAA Server Group:  CISCO_AD_SERVER
Group Member List Retrieved Successfully
Number of Members in AD Group group.schiang: 12
dn: CN=user1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
dn: CN=user2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
...
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。
show user-identity ad-groups	アイデンティティ ファイアウォールの AD エージェントに関する情報を表示します。

show user-identity ad-groups

アイデンティティ ファイアウォールの特定グループに関する情報を表示するには、特権 EXEC モードで **show user-identity ad-groups** コマンドを使用します。

show user-identity ad-groups *domain_nickname* {**filter** *filter_string* | **import-user-group** [**count**]}

構文の説明

count	(オプション)アクティブ化されたグループの数を表示します。
domain_nickname	アイデンティティ ファイアウォールのドメイン名を指定します。
filter *filter_string*	Microsoft Active Directory のドメイン コントローラの CN 属性に、指定したフィルタ文字列が含まれるグループを表示するように指定します。
import-user-group	アイデンティティ ファイアウォールのアクティブ化されたグループのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

show user-identity ad-groups コマンドを実行する場合、ASA は Microsoft Active Directory に LDAP クエリーを送信し、指定したドメイン ニックネームに含まれるすべてのユーザ グループを取得します。*domain_nickname* 引数には、実際のドメイン ニックネームまたは LOCAL を指定できます。ASA は、グループ オブジェクトクラス属性を持つグループのみを取得します。ASA は、取得したグループを distinguishedName 形式で表示します。

filter *filter_string* キーワードおよび引数を指定する場合、ASA は指定したフィルタ文字列をドメイン コントローラの CN 属性に含むグループを表示します。**access-list** および **object-group** コマンドは sAMAccountName のみを取得するため、**show user-identity ad-users filter** *filter_string* コマンドを実行してグループの sAMAccountName を取得できます。**filter** *filter_string* を指定しない場合、ASA はすべての Active Directory グループを表示します。

import-user-group count キーワードを指定している場合、ASA はアクティブ化され（アクセス グループ、インポート ユーザ グループ、またはサービス ポリシー コンフィギュレーションの一部であるため）、ローカル データベースに保存されているすべての Active Directory グループを表示します。ASA は、グループの sAMAccountName のみを表示します。

例

次に、アイデンティティ ファイアウォールに指定したドメイン ニックネームに含まれるユーザ グループを表示する例を示します。

```
ciscoasa# show user-identity ad-groups CSCO filter sampleuser1
Domain: CSCO        AAA Server Group:       CISCO_AD_SERVER
Group list retrieved successfully
Number of Active Directory Groups       6
dn: CN=group.reg.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.reg.sampleuser1
dn: CN=group.temp.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.temp.sampleuser1
...


ciscoasa# show user-identity ad-groups CSCO import-user-group count
Total AD groups in domain CSCO stored in local: 2


ciscoasa# show user-identity ad-groups CSCO import-user-group
Domain: CSCO
Groups:
        group.SampleGroup1
        group.SampleGroup2
...
```

次に、コマンドを実行して、access-list コマンドおよび object-group コマンドから結果にフィルタ文字列を適用する例を示します。**show user-identity ad-users CSCO filter SampleGroup1** コマンドを実行すると、指定した文字列の sAMAccountName が取得されます。

```
ciscoasa# show user-identity ad-users CSCO filter SampleGroup1
Domain:CSCO    AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 2
dn: CN=SampleUser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: SampleUser2
dn: CN=SAMPLEUSER2-WXP05,OU=Workstations,OU=Cisco Computers,DC=cisco,DC=com
sAMAccountName: SAMPLEUSER2-WXP05$
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity ad-users

アイデンティティ ファイアウォールの Microsoft Active Directory ユーザを表示するには、特権 EXEC モードで **show user-identity ad-users** コマンドを使用します。

show user-identity ad-users *domain_nickname* [**filter** *filter_string*]

構文の説明

domain_nickname	アイデンティティ ファイアウォールのドメイン名を指定します。
filter *filter_string*	（オプション）Microsoft Active Directory のドメイン コントローラの CN 属性に、指定したフィルタ文字列が含まれるユーザを表示するように指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

show user-identity ad-users コマンドを実行すると、ASA は Microsoft Active Directory に LDAP クエリーを送信し、指定したドメイン ニックネームに含まれるすべてのユーザを取得します。*domain_nickname* 引数には、実際のドメイン ニックネームまたは LOCAL を指定できます。

filter *filter_string* キーワードおよび引数を指定すると、ASA は指定したフィルタ文字列をドメイン コントローラの CN 属性に含むユーザを表示します。ASA は、Active Directory サーバで設定された Active Directory グループに対する LDAP クエリーを送信します。

ASA は、ユーザ オブジェクトクラス属性と samAccountType 属性 805306368 を持つユーザのみを取得します。マシン オブジェクトなどのその他のオブジェクトは、ユーザ オブジェクトクラスに含まれることがありますが、samAccountType 805306368 は非ユーザ オブジェクトを除外します。フィルタ文字列を指定しない場合、ASA はすべての Active Directory ユーザを表示します。

ASA は、取得したユーザを distinguishedName 形式で表示します。

例

次に、アイデンティティ ファイアウォールの Active Directory ユーザに関する情報を表示する例を示します。

```
ciscoasa# show user-identity ad-users CSCO filter user
Domain: CSCO        AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 10
dn: CN=sampleuser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser1
dn: CN=sampleuser2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser2
dn: CN=user3,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: user3
...
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity group

アイデンティティ ファイアウォール用に設定されたユーザ グループを表示するには、特権 EXEC モードで **show user-identity group** コマンドを使用します。

show user-identity group

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォール用に設定されたユーザ グループのトラブルシューティング情報を取得するには、**show user-identity group** コマンドを使用します。ASA は、Active Directory サーバで設定された Active Directory グループに対する LDAP クエリーを送信します。このコマンドは、アクティブ化されたユーザ グループのリストを次の形式で表示します。

*domain**group_name*

ASA は、セキュリティ ポリシーに適用される上位グループのみを表示します。アクティブ化された上位グループの最大数は 256 です。グループは、アクセス グループ、インポート ユーザ グループ、またはサービス ポリシー コンフィギュレーションの一部である場合にアクティブ化されます。

例

次に、アイデンティティ ファイアウォールのアクティブ化されたグループを表示する例を示します。

```
ciscoasa# show user-identity group
Group ID        Activated Group Name (Domain\\Group)
--------        ------------------------------------
       1        LOCAL\\og1
       2        LOCAL\\marketing
       3        CISCO\\group.sampleuser1
       4        IDFW\\grp1
...
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity ip-of-user

アイデンティティ ファイアウォールに指定したユーザの IP アドレスを表示するには、特権 EXEC モードで **show user-identity ip-of-user** コマンドを使用します。

show user-identity ip-of-user [*domain_nickname*\]*user-name* [**detail**]

構文の説明

detail	(オプション)ユーザおよび IP アドレスに関する詳細な出力を表示します。
domain_nickname	(オプション)アイデンティティ ファイアウォールのドメイン名を指定します。
user-name	IP アドレスを取得するユーザを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

このコマンドは、指定したユーザのユーザ情報と IP アドレスを表示します。1 ユーザに複数の IP アドレスが関連付けられている場合があります。

domain_nickname 引数を指定しない場合、ASA はデフォルト ドメインに *user_name* があるユーザの情報を表示します。*domain_nickname* 引数には、実際のドメイン ニックネームまたは LOCAL を指定できます。

detail キーワードを指定する場合、ASA は、指定したユーザ IP アドレスのすべてで、アクティブな接続の合計数、ユーザ統計情報の期間およびドロップ、期間中の入力パケットおよび出力パケットを表示します。**detail** オプションを指定しない場合、ASA は各 IP アドレスのドメイン ニックネームとステータスのみを表示します。

(注) ASA は、アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合にのみ、指定した期間の受信パケット、送信パケット、およびドロップなどの詳細なユーザ統計情報を表示します。アイデンティティ ファイアウォールの設定の詳細については、CLI 設定ガイドを参照してください。

例

次に、アイデンティティ ファイアウォールの指定したユーザの IP アドレスを表示する例を示します。

```
ciscoasa# show user-identity ip-of-user sampleuser1
CSCO\172.1.1.1 (Login)
CSCO\172.100.3.23 (Login)
CSCO\10.23.51.3 (Inactive)


ciscoasa# show user-identity ip-of-user sampleuser1 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 2 active conns
CSCO\172.100.3.23 (Login) Login time: 20 mins;  Idle time: 10 mins; 10 active conns
CSCO\10.23.51.3 (Inactive) Login time: 3000 mins;  Idle time: 2040 mins; 8 active conns
Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560


ciscoasa# show user-identity ip-of-user sampleuser2
ERROR: no such user


ciscoasa# show user-identity ip-of-user sampleuser3
ERROR: no IP address, user not login now
```

IPv6 サポート

```
ciscoasa# show user-identity ip-of-user sampleuser4
CSCO\172.1.1.1 (Login)
CSCO\8080:1:3::56 (Login)
CSCO\8080:2:3::34 (Inactive)


ciscoasa# show user-identity ip-of-user sampleuser4 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 8 active conns
CSCO\8080:1:3::56 (Login) Login time: 20 mins;  Idle time: 10 mins; 12 active conns
CSCO\8080:2:3::34 (Inactive) Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。
show user-identity user-of-ip	指定した IP アドレスに関連付けられたユーザ情報を表示します

show user-identity memory

アイデンティティ ファイアウォールの各種モジュールのメモリを表示するには、特権 EXEC モードで **show user-identity memory** コマンドを使用します。

show user-identity memory

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォールが ASA 上で消費するメモリ使用率をモニタできます。**show user-identity memory** コマンドを実行すると、ユーザ レコード、グループ レコード、ホスト レコード、およびそれらに関連するハッシュ テーブルのメモリが表示されます。ASA は、ID ベースの tmatch テーブルで使用されるメモリも表示します。

このコマンドは、アイデンティティ ファイアウォールの各種モジュールのメモリ使用率をバイト単位で表示します。

- ユーザ
- グループ
- User Statistics
- LDAP

ASA は、Active Directory サーバで設定された Active Directory グループに対する LDAP クエリーを送信します。Active Directory サーバは、ユーザを認証し、ユーザ ログオン セキュリティ ログを生成します。

- AD エージェント
- その他
- メモリ使用率合計

Identity Firewall で設定した AD エージェントからユーザ情報を取得する方法によって、この機能が使用するメモリの量が変わります。ASA がオン デマンド取得とフル ダウンロード取得のどちらを使用するかを指定します。オン デマンドを選択すると、受信パケットのユーザだけが取得および保存されるためにメモリの使用量が少なくなるというメリットがあります。これらのオプションの説明については、CLI 設定ガイドの「アイデンティティ オプションの設定」を参照してください。

例

次に、アイデンティティ ファイアウォールのモジュールのメモリ ステータスを表示する例を示します。

```
ciscoasa# show user-identity memory
Users:       22416048 bytes
Groups:           320 bytes
User stats:         0 bytes
LDAP:             300 bytes
AD agent:         500 bytes
Misc:           32428 bytes
Total:       22449596 bytes
Users:       22416048 bytes
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity statistics

アイデンティティ ファイアウォールのユーザまたはユーザ グループの統計情報を表示するには、特権 EXEC モードで **show user-identity statistics** コマンドを使用します。

show user-identity statistics [**user** [*domain_nickname*\]*user_name* | **user-group** [*domain_nickname*\]*user_group_name*]

構文の説明

domain_nickname	(オプション)アイデンティティ ファイアウォールのドメイン名を指定します。
user *user_name*	(オプション)統計情報を取得するユーザ名を指定します。
user-group *domain_nickname*\ *user_group_name*	(オプション)統計情報を取得するグループ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

ユーザまたはユーザ グループの統計情報を表示するには、**show user-identity statistics** コマンドを実行します。

domain_nickname 引数を **user** キーワードとともに指定しない場合、ASA はデフォルト ドメインに *user_name* があるユーザの情報を表示します。

domain_nickname を **user-group** キーワードとともに指定しない場合、ASA はデフォルト ドメインに *user_group_name* があるグループに関する情報を表示します。*domain_nickname* 引数には、実際のドメイン ニックネームまたは LOCAL を指定できます。

例

次に、アイデンティティ ファイアウォールのユーザに関する統計情報を表示する例を示します。

```
ciscoasa# show user-identity statistics user
Current monitored users:11  Total not monitored users:0
                          Average(eps)    Current(eps) Trigger      Total events
User: CSCO\user1 tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
  20-min Recv attack:                 4              10      14              4861
    1-hour Recv pkts:                   1              10        0              4901
User: CSCO\user2 tot-ses:2456 act-ses:607 fw-drop:0 insp-drop:0 null-ses:2431 bad-acc:0
  20-min Sent attack:                  4              10        4              4862
  1-hour Sent pkts:                      0               5         0              2451
...


ciscoasa# show user-identity statistics user user1
Current                           Average(eps)    Current(eps) Trigger      Total events
User: -(user1-) tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
  20-min Recv attack:                 4              10       14              4861
  1-hour Recv pkts:                    1              10       0              4901
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity statistics top user

アイデンティティ ファイアウォールの上位 10 ユーザの統計情報を表示するには、特権 EXEC モードで **show user-identity statistics top user** コマンドを使用します。

show user-identity statistics top user

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

show user-identity statistics top user コマンドは、上位 10 ユーザの受信した EPS パケット、送信した EPS パケット、および送信された攻撃に関する統計情報を表示します。(*domain\user_name* として表示される)各ユーザに関して、ASA は、そのユーザの平均 EPS パケット、現在の EPS パケット、トリガー、および合計イベント数を表示します。

例

次に、アイデンティティ ファイアウォールの上位 10 ユーザに関する情報を表示する例を示します。

```
ciscoasa# show user-identity statistics top user
Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv pkts:
01    APAC\sampleuser1
                                  0               0       0               391
  1-hour Sent pkts:
01    APAC\sampleuser2
                                  0               0       0               196
02    CSCO\sampleuser3
                                  0               0       0               195
  10-min Sent attack:
01    CSCO\sampleuser4
                                  0               0       0               352
02    CSCO\sampleuser3
                                  0               0       0               350
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity user active

アイデンティティ ファイアウォールのアクティブ ユーザを表示するには、特権 EXEC モードで **show user-identity user active** コマンドを使用します。

show user-identity user active [**domain** *domain_nickname* | **user-group** [*domain_nickname*\]*user_group_name* | **user** [*domain_nickname*\]*user_name*] [**list** [**detail**]]

構文の説明

detail	(オプション)アクティブ ユーザ セッションの詳細な出力を表示します。
domain *domain_nickname*	指定したドメインのアクティブ ユーザの統計情報を表示します。
list	(オプション)アクティブ ユーザの統計情報を要約したリストを表示します。
user *domain_nickname\user_name*	(オプション)指定したユーザの統計情報を表示します。
user-group *domain_nickname\user_group_name*	(オプション)指定したユーザ グループの統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォールで使用される IP/ユーザ マッピング データベースに含まれるすべてのユーザに関する情報を表示できます。

show user-identity user active コマンドは、ユーザに関する次の情報を表示します。

- *domain\user_name*
- Active Connections
- アイドル時間(分数)

デフォルトのドメイン名は、実際のドメイン名、特別な予約語、LOCAL のいずれかです。アイデンティティ ファイアウォールは、ローカルに定義されたすべてのユーザ グループまたはユーザ（VPN または Web ポータルを使用してログインおよび認証を行うユーザ）に対して LOCAL ドメイン名を使用します。デフォルト ドメインを指定しない場合、LOCAL がデフォルト ドメインとなります。

ユーザ名には、アイドル時間の数値が付加されます。ログイン時間およびアイドル時間は、ユーザの IP アドレスごとではなくユーザごとに保存されます。

user-group キーワードを指定した場合、アクティブ化されたユーザ グループのみが表示されます。グループは、アクセス グループ、インポート ユーザ グループ、またはサービス ポリシー コンフィギュレーションの一部である場合にアクティブ化されます。

domain_nickname を **user-group** キーワードとともに指定しない場合、ASA はデフォルト ドメインに *user_group_name* があるグループに関する情報を表示します。

（注） **user-identity action domain-controller-down** を **disable-user-identity-rule** キーワードとともに設定し、指定したドメインがダウンしているか、または **user-identity action ad-agent-down** コマンドを **disable-user-identity-rule** キーワードとともに設定し、AD エージェントがダウンしている場合は、ユーザ統計情報に、ログインしているすべてのユーザがディセーブルになっていると表示されます。

（注） ASA は、アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合にのみ、指定した期間の受信パケット、送信パケット、およびドロップなどの詳細なユーザ統計情報を表示します。アイデンティティ ファイアウォールの設定の詳細については、CLI 設定ガイドを参照してください。

例

次に、アイデンティティ ファイアウォールのアクティブ ユーザに関する情報を表示する例を示します。

```
ciscoasa# show user-identity user active
Total active users: 30  Total IP addresses: 35
  LOCAL: 0 users, 0 IP addresses
  cisco.com: 0 users, 0 IP addresses
  d1: 0 users, 0 IP addresses
  IDFW: 0 users, 0 IP addresses
  idfw.com: 0 users, 0 IP addresses
  IDFWTEST: 30 users, 35 IP addresses


ciscoasa# show user-identity user active domain CSCO
Total active users: 48020 Total IP addresses:10000
  CSCO: 48020 users, 10000 IP addresses


ciscoasa# show user-identity user active domain CSCO list
Total active users: 48020 Total IP addresses: 10000
  CSCO: 48020 users, 10000 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 5 mins
   CSCO\member-2: 20 active conns; idle 20 mins
   CSCO\member-3: 3 active conns; idle 101 mins
   …
```

```
ciscoasa# show user-identity user active list
Total active users: 48032  Total IP addresses: 10000
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 6 mins
   APAC\sampleuser2: 20 active conns; idle 0 mins
   CSCO\member-2: 20 active conns; idle 1 mins
   CSCO\member-3: 20 active conns; idle 0 mins
   APAC\member-2: 20 active conns; idle 22 mins
   CSCO\member-4: 3 active conns; idle 101 mins
   …
ciscoasa# show user-identity user active list detail
Total active users: 48032 Total IP addresses: 10010
  CSCO: 48020 users, 10000 IP addresses
  APAC: 12 users, 10 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
     172.1.1.1: login 360 mins, idle 0 mins, 15 active conns
     172.100.3.23: login 200 min, idle 15 mins , 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
   CSCO\member-1: 4 active connections;  idle 350 mins
   …
  APAC\sampleuser12: 3 active conns; idle 101 mins
     172.1.1.1: login 360 mins, idle 101 mins, 1 active conns
     172.100.3.23: login 200 min, idle 150 mins, 2 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560


ciscoasa# show user-identity user active list detail
Total users: 25  Total IP addresses: 5
   LOCAL\idfw: 0 active conns
    6.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
    20.0.0.3: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser4: 0 active conns; idle 0 mins
    20.0.0.2: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser5: 0 active conns
  ...


ciscoasa# show user-identity user active user sampleuser1 list detail
CSCO\sampleuser1: 20 active conns; idle 3 mins
     172.1.1.1: login 360 mins, idle 20 mins, 15 active conns
     172.100.3.23: login 200 mins, idle 3 mins, 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560


ciscoasa# show user-identity user active user APAC\sampleuser2
APAC\sampleuser2: 20 active conns; idle 2 mins


ciscoasa# show user-identity user active user-group APAC\\marketing list

   APAC\sampleuser1: 20 active conns; idle 2 mins
   APAC\member-1: 20 active conns; idle 0 mins
```

```
   APAC\member-2: 20 active conns; idle 0 mins
   APAC\member-3: 20 active conns; idle 6 mins
...

ciscoasa# show user-identity user active user-group APAC\\inactive list
ERROR: group is not activated
```

関連コマンド

コマンド	説明
clear user-identity active-user-database	アイデンティティ ファイアウォールの、指定したユーザ、指定したユーザ グループに属するすべてのユーザ、またはログアウトするすべてのユーザのステータスを設定します。
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity user all

アイデンティティ ファイアウォールのユーザに関する統計情報を表示するには、特権 EXEC モードで **show user-identity user all** コマンドを使用します。

show user-identity user all [**list**] [**detail**]

構文の説明

detail	(オプション)アイデンティティ ファイアウォールのすべてのユーザに関する詳細な出力を表示します。
list	(オプション)アイデンティティ ファイアウォールのすべてのユーザの統計情報を要約したリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォールで使用される IP ユーザ マッピング データベースに含まれるすべてのユーザの情報を表示するには、show user-identity all コマンドを使用します。

このコマンドとともに detail キーワードを指定し、コマンド出力に IP アドレスが非アクティブであると表示される場合、IP アドレスはユーザに関連付けられていません。その IP アドレスに関連付けられているユーザを検索するとエラーが返されます。

(注) **user-identity action domain-controller-down** を **disable-user-identity-rule** キーワードとともに設定し、指定したドメインがダウンしているか、または **user-identity action ad-agent-down** コマンドを **disable-user-identity-rule** キーワードとともに設定し、AD エージェントがダウンしている場合は、ユーザ統計情報に、ログインしているすべてのユーザがディセーブルになっていると表示されます。

(注) ASA は、アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合にのみ、指定した期間の受信パケット、送信パケット、およびドロップなどの詳細なユーザ統計情報を表示します。アイデンティティ ファイアウォールの設定の詳細については、CLI 設定ガイドを参照してください。

例

次に、アイデンティティ ファイアウォールのすべてのユーザに関する統計情報を表示する例を示します。

```
ciscoasa# show user-identity user all list
Total inactive users: 1201  Total IP addresses: 100


ciscoasa# show user-identity user all list
Total users: 7
  LOCAL\idfw: 0 active conns
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
  cisco.com\sampleuser4: 0 active conns; idle 300 mins
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
  cisco.com\sampleuser7: 0 active conns


ciscoasa# show user-identity user all list detail
Total users: 7 Total IP addresses: 3
  LOCAL\idfw: 0 active conns
    10.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns; idle 300 mins
    171.69.42.8: inactive
    10.0.0.2: login 300 mins, idle 300 mins, 5 active conns
  cisco.com\sampleuser4: 0 active conns
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity user inactive

アイデンティティ ファイアウォールの非アクティブユーザに関する情報を表示するには、特権 EXEC モードで **show user-identity user inactive** コマンドを使用します。

show user-identity user inactive [**domain** *domain_nickname* | **user-group** [*domain_nickname*\]*user_group_name*]

構文の説明

domain *domain_nickname*	(オプション)アイデンティティ ファイアウォールの指定したドメイン名にある非アクティブ ユーザの統計情報を表示します。
user-group *domain_nickname*\ *user_group_name*	(オプション)指定したユーザ グループの非アクティブ ユーザの統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

show user-identity user inactive コマンドを使用して設定した値よりも長い期間、アクティブ トラフィックがないユーザに関する情報を表示するには、**user-identity inactive-user-timer** コマンドを使用します。

user-group キーワードを指定した場合、アクティブ化されたユーザ グループのみが表示されます。グループは、アクセス グループ、インポート ユーザ グループ、またはサービス ポリシー コンフィギュレーションの一部である場合にアクティブ化されます。

domain_nickname を **user-group** キーワードとともに指定しない場合、ASA はデフォルト ドメインに *user_group_name* があるグループに関する情報を表示します。*domain_nickname* 引数には、実際のドメイン ニックネームまたは LOCAL を指定できます。

例

次に、アイデンティティ ファイアウォールの非アクティブ ユーザのステータスを表示する例を示します。

```
ciscoasa# show user-identity user inactive
Total inactive users: 1201
   APAC\sampleuser1
   CSCO\sampleuser2
172.1.1.1: inactive     …
...

ciscoasa# show user-identity user inactive domain CSCO
Total inactive users: 1101
    CSCO: 1101
   CSCO\sampleuser1
   CSCO\sampleuser2
   CSCO\sampleuser3
...


ciscoasa# show user-identity user inactive user-group CSCO\\marketing
Total inactive users: 21
   CSCO\sampleuser1
   CSCO\sampleuser2
...
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。
user-identity inactive-user-timer	ユーザを Cisco アイデンティティ ファイアウォール インスタンスのアイドル状態と見なすまでの時間を指定します。

show user-identity user-not-found

アイデンティティ ファイアウォールの見つからない Active Directory ユーザの IP アドレスを表示するには、特権 EXEC モードで **show user-identity user-not-found** コマンドを使用します。

show user-identity user-not-found

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

Microsoft Active Directory で見つからないユーザの IP アドレスを表示するには、**show user-identity user-not-found** コマンドを使用します。

ASA は、これらの IP アドレスのローカルの user-not-found データベースを保持します。ASA は、データベースのリスト全体ではなく、user-not-found リストの最後の 1024 パケットのみを保持します（同じ送信元 IP アドレスからの連続するパケットは 1 つのパケットとして扱われます）。

例

次に、アイデンティティ ファイアウォールの not-found ユーザに関する情報を表示する例を示します。

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
…
```

関連コマンド

コマンド	説明
clear user-identity user-not-found	アイデンティティ ファイアウォールの ASA のローカル user-not-found データベースをクリアします。
user-identity enable	Cisco Identity Firewall インスタンスを作成します。
user-identity user-not-found	アイデンティティ ファイアウォールの user-not-found トラッキングをイネーブルにします。

show user-identity user-of-group

アイデンティティ ファイアウォールの指定したユーザ グループのユーザを表示するには、特権 EXEC モードで **show user-identity user-of-group** コマンドを使用します。

show user-identity user-of-group [*domain_nickname*\]*user_group_name*

構文の説明

domain_nickname	アイデンティティ ファイアウォールのドメイン名を指定します。
user_group_name	統計情報を表示するユーザ グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

グループ ID が指定したユーザ グループに一致するユーザを表示するには、**show user-identity user-of-group** コマンドを使用します(ASA は、LDAP クエリーを Active Directory に送信するのではなく、この情報の IP ユーザ ハッシュ リストをスキャンします。AD エージェントは、ユーザ ID および IP アドレス マッピングのキャッシュを保持し、ASA に変更を通知します)。

名前を指定するユーザ グループはアクティブ化されている必要があります。グループはインポート ユーザ グループ(アクセス リストまたはサービス ポリシー コンフィギュレーションのユーザ グループとして定義)またはローカル ユーザ グループ(オブジェクト グループ ユーザとして定義)です。

グループは、複数のユーザ メンバーを持つことができます。ユーザ グループのメンバーは、すべて、指定したグループの直近メンバー(ユーザとグループを含む)です。

domain_nickname を *user_group_name* 引数とともに指定しない場合、ASA はデフォルト ドメインに *user_group_name* があるグループに関する情報を表示します。*domain_nickname* 引数には、実際のドメイン ニックネームまたは LOCAL を指定できます。

コマンド出力にユーザ ステータスが非アクティブであると表示される場合、ユーザはログアウトしているか、一度もログインしていません。

例

次に、アイデンティティ ファイアウォールの指定したユーザ グループのユーザを表示する例を示します。

```
ciscoasa# show user-identity user-of-group group.samplegroup1
Group: CSCO\\group.user1 Total users: 13
CSCO\user2 10.0.0.10(Login) 20.0.0.10(Inactive) …
CSCO\user3 10.0.0.11(Inactive)
CSCO\user4 10.0.0.12 (Login)
CSCO\user5 10.0.0.13 (Login)
CSCO\user6 10.0.0.14 (Inactive)
....


ciscoasa# show user-identity user-of-group group.local1
Group: LOCAL\\group.local1    Total users: 2
CSCO\user1 10.0.4.12 (Login)
LOCAL\user2 10.0.3.13 (Login)
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show user-identity user-of-ip

アイデンティティ ファイアウォールの特定 IP アドレスを使用するユーザに関する情報を表示するには、特権 EXEC モードで **show user-identity user-of-ip** コマンドを使用します。

show user-identity user-of-ip *ip_address* [**detail**]

構文の説明

detail	(オプション)指定した IP アドレスを使用するユーザに関する詳細な出力を表示します。
ip_address	情報を表示するユーザの IP アドレスを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	コマンドが追加されました。

使用上のガイドライン

指定した IP アドレスに関連付けられたユーザ情報を表示するには、**show user-identity user-of-ip** コマンドを使用します。

detail キーワードを指定する場合、ASA は、ユーザ ログイン時間、アイドル時間、アクティブな接続数、ユーザ統計情報の期間とドロップ、および期間中の入力パケットと出力パケットを表示します。**detail** キーワードを指定しない場合、ASA はドメイン ニックネーム、ユーザ名、およびステータスのみを表示します。

ユーザ ステータスが非アクティブな場合、ユーザはログアウトしているか、一度もログインしていません。

このコマンドとともに **detail** キーワードを指定し、IP アドレスのコマンド出力にエラーが表示される場合、IP アドレスは非アクティブです。つまり、IP アドレスがユーザに関連付けられていません。

(注) ASA は、アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合にのみ、指定した期間の受信パケット、送信パケット、およびドロップなどの詳細なユーザ統計情報を表示します。アイデンティティ ファイアウォールの設定の詳細については、CLI 設定ガイドを参照してください。

例

次に、アイデンティティ ファイアウォールのアクティブ ユーザのステータスを表示する例を示します。

```
ciscoasa# show user-identity user-of-ip 172.1.1.1
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 172.1.1.1 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 172.1.2.2 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 172.1.7.7
ERROR: no user with this IP address
```

IPv6 のサポート

```
ciscoasa# show user-identity user-of-ip 8080:1:1::4
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 8080:1:1::4 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 8080:1:1::6 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60

ciscoasa# show user-identity user-of-ip 8080:1:1::100
ERROR: no user with this IP address
```

関連コマンド

コマンド	説明
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

show version

ソフトウェア バージョン、ハードウェア構成、ライセンス キー、および関連する動作期間データを表示するには、ユーザ EXEC モードで **show version** コマンドを使用します。

show version

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	ステートフル フェールオーバー モードでは、クラスタの動作期間を示す追加の行が表示されます。
8.3(1)	出力に、機能で使用されるのが永続キーまたは時間ベース キーのいずれであるか、および使用中の時間ベース キーの期間が含まれるようになりました。
8.4(1)	ペイロード暗号化機能のないモデル（NPE）のサポートが追加されました。
9.3(2)	REST API エージェントがイネーブルの場合、バージョン番号が表示されます。

使用上のガイドライン

show version コマンドを使用すると、ソフトウェア バージョン、最後にリブートされてからの動作時間、プロセッサ タイプ、フラッシュ パーティション タイプ、インターフェイス ボード、シリアル番号（BIOS ID）、アクティベーション キー値、ライセンス タイプ、およびコンフィギュレーションが最後に変更されたときのタイムスタンプを表示できます。

REST API エージェントがインストールされ、イネーブルになっている場合、バージョン番号も表示されます。

show version コマンドで表示されるシリアル番号は、フラッシュ パーティション BIOS の番号です。この番号は、シャーシのシリアル番号とは異なります。ソフトウェア アップグレードを入手する場合は、シャーシ番号ではなく、**show version** コマンドで表示されるシリアル番号が必要です。

フェールオーバー クラスタの動作期間の値は、フェールオーバー セットが動作している期間の長さを示しています。1 台のユニットが動作を停止しても、アクティブなユニットが動作を継続する限り、動作期間の値は増加し続けます。このため、フェールオーバー クラスタの動作期間を個別のユニットの動作期間よりも長くすることができます。フェールオーバーを一時的にディセーブルにしてから再びイネーブルにすると、フェールオーバーがディセーブルになる前のユニットの稼働時間と、フェールオーバーがディセーブルである間のユニットの稼働時間が加算されて、フェールオーバー クラスタの動作期間がレポートされます。

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN およびユニファイド コミュニケーション ライセンスはリストに示されません。

ASA 5505 の合計 VPN ピアの場合、すべてのタイプの VPN セッションの合計数はライセンスによって異なります。AnyConnect Essentials をイネーブルにしている場合、合計はモデルの最大数の 25 です。AnyConnect Premium をイネーブルにしている場合、合計は AnyConnect Premium 値にその他の VPN 値を加えた、25 セッションを超えないものとなります。その他の VPN 値がすべての VPN セッションのモデル制限と等しい他のモデルとは異なり、ASA 5505 のその他の VPN 値はモデル制限よりも低いため、合計値は AnyConnect Premium ライセンスによって変わることがあります。

例

次に、**show version** コマンドの出力例を示します。この例では、ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示する方法を示しています。ステートフル フェールオーバーが設定されている環境では、フェールオーバー クラスタの動作期間を示す追加の行が表示されます。フェールオーバーが設定されていない場合、この行は表示されません。この表示は、最小メモリ要件に関する警告メッセージを示します。

```
**************************************************************************
**                                                                      **
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***    **
**                                                                      **
**          ----> Minimum Memory Requirements NOT Met! <----            **
**                                                                      **
**  Installed RAM:  512 MB                                              **
**  Required  RAM: 2048 MB                                              **
**  Upgrade part#: ASA5520-MEM-2GB=                                     **
**                                                                      **
**  This ASA does not meet the minimum memory requirements needed to    **
**  run this image. Please install additional memory (part number       **
**  listed above) or downgrade to ASA version 8.2 or earlier.           **
**  Continuing to run without a memory upgrade is unsupported, and      **
**  critical system features will not function properly.                **
**                                                                      **
**************************************************************************

Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)

Compiled on Thu 20-Jan-12 04:05 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/tomm_backup.cfg"

asa3 up 3 days 3 hours

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 128MB
BIOS Flash AT49LW080 @ 0xfff00000, 1024KB
```

```
Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.06
 0: Ext: GigabitEthernet0/0  : address is 0013.c480.82ce, irq 9
 1: Ext: GigabitEthernet0/1  : address is 0013.c480.82cf, irq 9
 2: Ext: GigabitEthernet0/2  : address is 0013.c480.82d0, irq 9
 3: Ext: GigabitEthernet0/3  : address is 0013.c480.82d1, irq 9
 4: Ext: Management0/0       : address is 0013.c480.82cd, irq 11
 5: Int: Not used            : irq 11
 6: Int: Not used            : irq 5

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.
The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days

Serial Number: JMX0938K0C0
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Configuration register is 0x1
Configuration last modified by docs at 15:23:22.339 EDT Fri Oct 30 2012
```

eject コマンドを実行した後、デバイスが物理的に取り外されていない状態で **show version** コマンドを入力すると、次のメッセージが表示されます。

```
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
```

関連コマンド

コマンド	説明
eject	ASA から物理的に取り外す前に外部コンパクト フラッシュ デバイスをシャットダウンできるようにします。
show hardware	ハードウェアの詳細情報を表示します。
show serial	ハードウェアのシリアル情報を表示します。
show uptime	ASA の稼働時間を表示します。

show vlan

ASA に設定されているすべての VLAN を表示するには、特権 EXEC モードで **show vlan** コマンドを使用します。

show vlan [**mapping** [*primary_id*]]

構文の説明

マッピング	(オプション)プライマリ VLAN にマッピングされたセカンダリ VLAN を表示します。
primary_id	(オプション)特定のプライマリ VLAN のセカンダリ VLAN を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.5(2)	**mapping** キーワードが追加されました。

例

次に、設定されている VLAN を表示する例を示します。

```
ciscoasa# show vlan
10-11,30,40,300
```

次に、各プライマリ VLAN にマッピングされたセカンダリ VLAN を表示する例を示します。

```
ciscoasa# show vlan mapping
Interface                   Secondary VLAN ID                   Mapped VLAN ID
0/1.100                     200                                         300
0/1.100                     201                                         300
0/2.500                     400                                         200
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show vm

ASAv の仮想プラットフォーム情報を表示するには、特権 EXEC モードで **show vm** コマンドを使用します。

show vm

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASAv に関して、次のライセンス ガイドラインに注意してください。

- 許可される vCPU の数は、インストールされている vCPU プラットフォーム ライセンスによって決定されます。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数と一致する場合、状態は Compliant になります。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数を下回る場合、状態は Noncompliant: Over-provisioned になります。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数を超える場合、状態は Compliant: Under-provisioned になります。
- メモリ制限は、プロビジョニングされた vCPU の数によって決定されます。
  - プロビジョニングされたメモリが上限にある場合、状態は Compliant になります。
  - プロビジョニングされたメモリが上限を超える場合、状態は Noncompliant: Over-provisioned になります。
  - プロビジョニングされたメモリが上限を下回る場合、状態は Compliant: Under-provisioned になります。

- 周波数予約制限は、プロビジョニングされた vCPU の数によって決定されます。
  - 周波数予約メモリが必要最低限（1000 MHz）以上である場合、状態は Compliant になります。
  - 周波数予約メモリが必要最低限（1000 MHz）未満である場合、状態は Compliant: Under-provisioned になります。

例

次に、ライセンスなしの ASAv10 に関する仮想プラットフォーム情報を表示する例を示します。

```
ciscoasa# show vm

Virtual Platform Resource Limits
--------------------------------
Number of vCPUs              :     0
Processor Memory             :     0 MB

Virtual Platform Resource Status
--------------------------------
Number of vCPUs                 :     1     (Noncompliant: Over-provisioned)
Processor Memory                :  2048 MB  (Noncompliant: Over-provisioned)
Hypervisor                      :   VMware
Model Id                        :   ASAv10
```

次に、ライセンス付き ASAv10 に関する仮想プラットフォーム情報を表示する例を示します。

```
ciscoasa# show vm

Virtual Platform Resource Limits
--------------------------------
Number of vCPUs              :     1
Processor Memory             :  2048 MB

Virtual Platform Resource Status
--------------------------------
Number of vCPUs                 :     1     (Compliant)
Processor Memory                :  2048 MB  (Compliant)
Hypervisor                      :   VMware
Model Id                        :   ASAv10
```

関連コマンド

コマンド	説明
show cpu detail	vCPU ごとに vCPU 情報を表示します。

show vni vlan-mapping

VNI セグメント ID と VLAN インターフェイスまたは物理インターフェイスとの間のマッピングを表示するには、特権 EXEC モードで **show vni vlan-mapping** コマンドを使用します。

show vni vlan-mapping

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ルーテッド モードでは、VXLAN と VLAN 間のマッピングに表示する値を大量に含めることができるため、トランスペアレント ファイアウォール モードでのみ有効です。

例

show vni vlan-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3, interface:
'g112', vlan 4
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。

コマンド	説明
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレス テーブル）を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

show vpdn

PPPoE または L2TP のような仮想プライベート ダイヤルアップ ネットワーク（VPDN）接続のステータスを表示するには、特権 EXEC モードで **show vpdn** コマンドを使用します。

show vpdn {**group** *name* | **pppinterface** [**id** *number*] | **session** [**l2tp** | **pppoe**] [**id** *number*] {**packets** | **state** | **window**} | **tunnel** [**l2tp** | **pppoe**] [**id** *number*] {**packets** | **state** | **summary** | **transport**} | **username** *name*}

構文の説明

group *name*	VPDN グループのコンフィギュレーションを表示します。
id *number*	（オプション）指定された ID を持つ VPDN セッションに関する情報を表示します。
l2tp	（オプション）L2TP に関するセッションまたはトンネルの情報を表示します。
パケット	セッションまたはトンネル パケットの情報を表示します。
pppinterface	PPP インターフェイス情報を表示します。
pppoe	（オプション）PPPoE に関するセッションまたはトンネルの情報を表示します。
session	セッション情報を表示します。
state	セッションまたはトンネルの状態の情報を表示します。
summary	トンネルの概要を表示します。
transport	トンネルのトランスポート情報を表示します。
tunnel	トンネル情報を表示します。
username *name*	ユーザ情報を表示します。
window	セッション ウィンドウ情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

VPDN PPPoE 接続または L2TP 接続をトラブルシューティングするには、このコマンドを使用します。

例

次に、**show vpdn session** コマンドの出力例を示します。

```
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

次に、**show vpdn tunnel** コマンドの出力例を示します。

```
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
```

関連コマンド

コマンド	説明
vpdn group	VPDN クライアント設定を行います。

show vpn cluster stats internal

VPN クラスタリングの内部カウンタを表示するには、グローバル設定または特権 EXEC モードでこのコマンドを使用します。

show vpn cluster stats internal

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.9(1)	コマンドが追加されました。

関連コマンド

コマンド	説明
clear vpn cluster stats internal	すべての VPN クラスタ カウンタをクリアします。

show vpn load-balancing

VPN ロード バランシングの仮想クラスタ コンフィギュレーションに関する実行時統計情報を表示するには、グローバル コンフィギュレーション モード、特権 EXEC モード、または VPN ロード バランシング モードで **show vpn-load-balancing** コマンドを使用します。

show vpn load-balancing

構文の説明

このコマンドには、変数も引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—
VPN ロード バランシング	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	出力例の Load (%) 表示および Session 表示に、個別の IPsec 列および SSL 列が追加されました。
8.4(2)	表示される出力に新しい情報が追加されました。

使用上のガイドライン

show vpn load-balancing コマンドは、仮想 VPN ロード バランシング クラスタに関する統計情報を表示します。ローカル デバイスが VPN ロード バランシング クラスタに参加していない場合、このコマンドはデバイスに VPN ロード バランシングが設定されていないことを通知します。

出力にあるアスタリスク (*) は、接続先の ASA の IP アドレスを示します。

例

次に、ローカル デバイスが VPN ロード バランシング クラスタに参加してい場合の **show vpn load-balancing** コマンドの出力例を示します。

```
ciscoasa# sh vpn load-balancing
------------------------------------------------------------------------------
    Status     Role    Failover    Encryption        Cluster IP    Peers
```

```
-------------------------------------------------------------------------
   Enabled   Master        n/a     Disabled 192.0.2.255   0

Peers:
-------------------------------------------------------------------------
       Public IP     Role  Pri             Model  Load-Balancing Version
-------------------------------------------------------------------------
       192.0.2.255    Master    5          ASA-5520            3

Total License Load:
-------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials          Other VPN
                    -----------------------------   ---------------------
                        Limit    Used   Load          Limit    Used   Load
-------------------------------------------------------------------------
     192.0.2.255       750       0     0%            750       1     0%

Licenses Used By Inactive Sessions :
-------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials     Inactive Load
-------------------------------------------------------------------------
     192.0.2.255                      0                0%
```

プライマリ デバイスでは、[Total License Load] 出力にプライマリおよびバックアップ デバイスに関する情報が示されます。ただし、バックアップ デバイスは、プライマリ デバイスではなく自身に関する情報のみを表示します。したがって、プライマリ デバイスはすべてのライセンス メンバーを認識しますが、ライセンス メンバーは自身のライセンスのみを認識します。

出力には、[License Used by Inactive Session] セクションも含まれます。AnyConnect セッションが非アクティブになる場合、ASA はセッションが正常な手段で終了されていなければそのセッションを保持します。そのように、AnyConnect セッションは同じ webvpn クッキーを使用して再接続できます。再認証する必要はありません。非アクティブなセッションは、AnyConnect クライアントがセッションを再開するかアイドル タイムアウトが発生するまで、その状態のままになります。セッションのライセンスは、これらの非アクティブなセッションのために保持され、この [License Used by Inactive Session] セクションに示されます。

ローカル デバイスが VPN ロード バランシング クラスタに参加していない場合、**show vpn load-balancing** コマンドには次のような異なる結果が表示されます。

```
ciscoasa(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	コンフィギュレーションから **vpn load-balancing** コマンド ステートメントを削除します。
show running-config vpn load-balancing	現在の VPN ロード バランシング仮想クラスタのコンフィギュレーションを表示します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

show vpn-sessiondb

VPN セッションに関する情報を表示するには、特権 EXEC モードで **show vpn-sessiondb** コマンドを使用します。このコマンドには、すべての情報または詳細な情報を表示するためのオプションがあり、表示するセッションのタイプを指定できます。また、情報をフィルタリングおよびソートするためのオプションも用意されています。構文の表と使用上の注意で、使用可能なオプションについてそれぞれ説明しています。

show vpn-sessiondb [all] [backup {index | l2l}] [detail] [ospfv3] [failover] [full] [summary] [ratio {encryption | protocol}] [license-summary] {anyconnect | email-proxy | index *indexnumber* **| l2l | ra-ikev1-ipsec | ra-ikev2-ipsec | vpn-lb | webvpn} [filter {name** *username* **| ipaddress** *IPaddr* **| a-ipaddress** *IPaddr* **| p-ipaddress** *IPaddr* **| tunnel-group** *groupname* **| protocol** *protocol-name* **| encryption** *encryption-algo* **| inactive}] [sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption | inactivity}]**

構文の説明

all	アクティブとバックアップのすべてのクラスタ セッションを表示します。
anyconnect	OSPFv3 セッション情報を含む AnyConnect VPN クライアント セッションを表示します。
backup {index | l2l}	バックアップ セッションのみを表示します。
detail	(任意)セッションに関する詳細情報を表示します。たとえば、IPsec セッションに対して **detail** オプションを使用すると、IKE ハッシュ アルゴリズム、認証モード、キー再生成間隔などの詳細情報が表示されます。 **detail** および **full** オプションを指定すると、ASA ではマシンで読み取り可能な形式で詳細な出力を表示します。
email-proxy	(廃止予定)電子メールプロキシ セッションを表示します。
encryption	セッション合計数の比率として暗号化タイプの比率を表示します。
failover	フェールオーバー IPSec トンネルのセッション情報を表示します。
filter *filter_criteria*	(任意)1 つまたは複数のフィルタ オプションを使用して、指定する情報だけを表示するように出力をフィルタリングします。*filter_criteria* オプションのリストについては、「使用上のガイドライン」を参照してください。
full	(任意)連続した、短縮されていない出力を表示します。出力のレコード間には | 文字と || ストリングが表示されます。
index *indexnumber*	インデックス番号を指定して、単一のセッションを表示します。セッションのインデックス番号を指定します。範囲は 1 ～ 750 です。
l2l	VPN の LAN-to-LAN セッション情報を表示します。 detail を選択しているときには、クラスタの情報も提供されます。
license-summary	VPN ライセンス サマリー情報を表示します。
ospfv3	OSPFv3 セッション情報を表示します。
protocol	セッション合計数の比率としてプロトコル タイプの比率を表示します。
ra-ikev1-ipsec	IPsec IKEv1 セッションを表示します。
ra-ikev2-ipsec	IKEv2 リモート アクセス クライアント接続の詳細を表示します。
sort *sort_criteria*	(任意)指定するソート オプションに従って出力をソートします。*sort_criteria* オプションのリストについては、「使用上のガイドライン」を参照してください。

summary	VPN セッション サマリー情報を表示します。
vpn-lb	VPN ロード バランシングの管理セッションを表示します。
webvpn	OSPFv3 セッション情報を含むクライアントレス SSL VPN セッションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	VLAN フィールドの説明が追加されました。
8.0(5)	**inactive** が **filter** オプションとして、**inactivity** が **sort** オプションとして追加されました。
8.2(1)	ライセンス情報が出力に追加されました。
8.4(1)	**svc** キーワードが **anyconnect** に変更されました。**remote** キーワードが **ra-ikev1-ipsec** に変更されました。**ratio** キーワードが追加されました。
9.0(1)	**ospfv3** キーワードが追加され、OSPFv3 セッション情報が VPN セッションのサマリーに含まれるようになりました。 **filter a-ipversion** オプションおよび **filter p-ipversion** オプションが追加され、IPv4 アドレスまたは IPv6 アドレスが割り当てられたすべての AnyConnect、LAN-to-LAN、およびクライアントレス SSL VPN のセッションでフィルタリングできるようになりました。 マルチ コンテキスト モードのサポートが追加されました。
9.1(2)	フェールオーバー IPsec トンネルをサポートするフェールオーバー トンネル タイプと **failover** キーワードが追加されました。**failover ipsec pre-shared-key** コマンドを参照してください。
9.1(4)	割り当てられた IPv6 アドレスを反映し、IKEv2 デュアル トラフィックの実行時に GRE トランスポート モードのセキュリティ アソシエーションを示すように、**detail anyconnect** オプションを使用する場合の出力が更新されました。

リリース	変更内容
9.3(2)	IKEv2 リモート アクセス クライアント接続の詳細を表示する **ra-ikev2-ipsec** キーワードが追加されました。IKEv2 リモート アクセス クライアント接続および IKEv2 および IPsec トンネル カウントを含めるように、VPN セッションのサマリー出力が更新されました。IKEv2 リモート アクセス クライアント接続を追加するように、VPN ライセンスの使用状況のサマリー出力が更新されました。
9.4(1)	このコマンドの出力に、Cert Auth Int と Cert Auth Left が追加されました。
9.8(1)	**email-proxy** オプションが廃止されました。
9.9(1)	**all** および **backup** オプションが追加されました。

使用上のガイドライン

次のオプションを使用して、セッションに関する表示内容をフィルタリングおよびソートできます。

フィルタ/ソート オプション	説明
filter a-ipaddress *IPaddr*	出力をフィルタリングして、指定した割り当て済み IP アドレス（複数可）に関する情報だけを表示します。
sort a-ipaddress	割り当て済み IP アドレスで表示内容をソートします。
filter a-ipversion {v4 | v6}	出力をフィルタリングして、IPv4 または IPv6 アドレスを割り当てられたすべての AnyConnect セッションに関する情報を表示します。
filter encryption *encryption-algo*	出力をフィルタリングして、指定した暗号化アルゴリズム（複数可）を使用しているセッションに関する情報だけを表示します。
sort encryption	暗号化アルゴリズムで表示内容をソートします。暗号化アルゴリズムには、aes128、aes192、aes256、des、3des、rc4 が含まれます。
filter inactive	アイドル状態であり、（ハイバネーション、モバイル デバイス切断などによって）接続が切断された可能性がある非アクティブなセッションをフィルタリングします。非アクティブなセッションの数は、TCP キープアライブが AnyConnect クライアントから応答なしで ASA から送信されると増加します。各セッションには、SSL トンネルがドロップした時間でタイムスタンプが付けられます。セッションが SSL トンネルを介してアクティブにトラフィックを渡している場合、00:00m:00s が表示されます。 （注） ASA は、バッテリ寿命を節約するために一部のデバイス（iPhone、iPad、iPod など）に TCP キープアライブを送信しないため、障害検出は切断とスリープを区別できません。そのため、非アクティブなカウンタは設計によって 00:00:00 のままになります。
sort inactivity	非アクティブなセッションをソートします。
filter ipaddress *IPaddr*	出力をフィルタリングして、指定した内部 IP アドレス（複数可）に関する情報だけを表示します。
sort ipaddress	内部 IP アドレスで表示内容をソートします。

フィルタ/ソート オプション	説明
filter name *username*	出力をフィルタリングして、指定したユーザ名（複数可）のセッションを表示します。
sort name	ユーザ名のアルファベット順に表示内容をソートします。
filter p-address *IPaddr*	出力をフィルタリングして、指定した外部 IP アドレスに関する情報だけを表示します。
sort p-address	指定した外部 IP アドレス（複数可）で表示内容をソートします。
filter p-ipversion {v4 | v6}	出力をフィルタリングして、IPv4 または IPv6 アドレスを割り当てられたエンドポイントから送信されるすべての AnyConnect セッションに関する情報を表示します。
filter protocol *protocol-name*	出力をフィルタリングして、指定したプロトコル（複数可）を使用しているセッションに関する情報だけを表示します。
sort protocol	プロトコルで表示内容をソートします。プロトコルには、IKE、IMAP4S、IPsec、IPsecLAN2LAN、IPsecLAN2LANOverNatT、IPsecOverNatT、IPsecoverTCP、IPsecOverUDP、SMTPS、userHTTPS、vcaLAN2LAN が含まれます。
filter tunnel-group *groupname*	出力をフィルタリングして、指定したトンネル グループ（複数可）に関する情報だけを表示します。
sort tunnel-group	トンネル グループで表示内容をソートします。
|	引数 {begin | include | exclude | grep | [-v]} {reg_exp} を使用して、出力を修正します。

注：コマンド出力には、最大 120 文字のユーザ名のみが表示されます。120 文字を超える場合、超えた分の文字を切り捨ててコマンド出力に表示されます。

例

次に、**show vpn-sessiondb** コマンドの出力例を示します。

```
ciscoasa# show vpn-sessiondb

--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ----------------------------------------------
AnyConnect Client            :      1 :         78 :           2 :        0
  SSL/TLS/DTLS               :      1 :         72 :           2 :        0
  IKEv2 IPsec                :      0 :          6 :           1 :        0
IKEv2 Generic IPsec Client   :      0 :          0 :           0
Clientless VPN               :      0 :          8 :           2
  Browser                    :      0 :          8 :           2
--------------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :     86
Device Total VPN Capacity    :    750
Device Load                  :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
```

```
IKEv2                         :      0 :          6 :               1
IPsecOverNatT                 :      0 :          6 :               1
Clientless                    :      0 :         17 :               2
AnyConnect-Parent             :      1 :         69 :               2
SSL-Tunnel                    :      1 :         75 :               2
DTLS-Tunnel                   :      1 :         56 :               2
------------------------------------------------------------------------------
Totals                        :      3 :        229
------------------------------------------------------------------------------

------------------------------------------------------------------------------
IPv6 Usage Summary
------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ------------------------------------------
AnyConnect SSL/TLS/DTLS       :        :            :
  IPv6 Peer                   :      1 :         41 :           2
  Tunneled IPv6               :      1 :         70 :           2
AnyConnect IKEv2              :        :            :
  IPv6 Peer                   :      0 :          4 :           1
Clientless                    :        :            :
  IPv6 Peer                   :      0 :          1 :           1
------------------------------------------------------------------------------
```

次に、**show vpn-sessiondb detail l2l** コマンドの出力例を示します。LAN-to-LAN セッションに関する詳細情報が表示されています。

```
ciscoasa# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed

Connection   : 172.16.0.0
Index        : 1
IP Addr      : 172.16.0.0
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 240                    Bytes Rx     : 160
Login Time   : 14:50:35 UTC Tue May 1 2012
Duration     : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 1.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86389 Seconds
  PRF          : SHA1                   D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :

IPsec:
  Tunnel ID    : 1.2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                 Hashing      : SHA1
  Encapsulation: Tunnel                 PFS Group    : 5
  Rekey Int (T): 120 Seconds            Rekey Left(T): 107 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
```

```
  Bytes Tx     : 240                    Bytes Rx     : 160
  Pkts Tx      : 3                      Pkts Rx      : 2

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 13 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

次に、**show vpn-sessiondb detail index 1** コマンドの出力例を示します。

```
AsaNacDev# show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username     : user1
Index        : 1
Assigned IP  : 192.168.2.70           Public IP    : 10.86.5.114
Protocol     : IPsec                  Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                      Bytes Rx     : 604533
Client Type  : WinNT                  Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy
VM Result    : Static
VLAN         : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 61078 Seconds
  D/H Group    : 2

IPsec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                      Bytes Rx     : 604533
  Pkts Tx      : 0                      Pkts Rx      : 8126

NAC:
  Reval Int (T): 3000 Seconds           Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds            EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds              Posture Token: Healthy
  Redirect URL : www.cisco.com
```

次に、**show vpn-sessiondb ospfv3** コマンドの出力例を示します。

```
asa# show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec

Connection   :
Index        : 1                      IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none         Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:13m:11s
```

次に、**show vpn-sessiondb detail ospfv3** コマンドの出力例を示します。

```
asa# show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection   :
Index        : 1                      IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none         Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
  Tunnel ID    : 1.1
  Local Addr   : ::/0/89/0
  Remote Addr  : ::/0/89/0
  Encryption   : none                   Hashing      : SHA1
  Encapsulation: Transport
  Idle Time Out: 0 Minutes              Idle TO Left : 0 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 0
  Pkts Tx      : 0                      Pkts Rx      : 0

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 105268 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

次に、**show vpn-sessiondb summary** コマンドの出力例を示します。

```
ciscoasa# show vpn-sessiondb summary
-------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
OSPFv3 IPsec                :      1 :          1 :           1
-------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :      1
Device Total VPN Capacity    :  10000
Device Load                  :     0%
-------------------------------------------------------------------------
```

次に、一般的な IKEv2 IPsec リモート アクセス セッションの **show vpn-sessiondb summary** コマンドの出力例を示します。

```
ciscoasa# show vpn-sessiondb summary
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                              Active : Cumulative : Peak Concur : Inactive
                             ------------------------------------------
Generic IKEv2 Remote Access  :      1 :          1 :           1
----------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :      1
Device Total VPN Capacity    :    250
Device Load                  :     0%
----------------------------------------------------------------------------

----------------------------------------------------------------------------
Tunnels Summary
----------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ------------------------------------------
IKEv2                        :      1 :          1 :               1
IPsec                        :      1 :          1 :               1
----------------------------------------------------------------------------
Totals                       :      2 :          2
----------------------------------------------------------------------------
```

次に、**show vpn-sessiondb det anyconnect** コマンドの出力例を示します。

```
ciscoasa# show vpn-sessiondb det anyconnect

Session Type: AnyConnect Detailed

Username     : userab                 Index        : 2
Assigned IP  : 65.2.1.100             Public IP    : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : IKEv2: (1)3DES  IPsecOverNatT: (1)3DES  AnyConnect-Parent: (1)none
Hashing      : IKEv2: (1)SHA1  IPsecOverNatT: (1)SHA1  AnyConnect-Parent: (1)none
Bytes Tx     : 0                      Bytes Rx     : 21248
Pkts Tx      : 0                      Pkts Rx      : 238
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : test1
Login Time   : 22:44:59 EST Tue Aug 13 2013
Duration     : 0h:02m:42s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 75.2.1.60
  Encryption   : none                   Hashing      : none
  Auth Mode    : userPassword
  Idle Time Out: 400 Minutes            Idle TO Left : 397 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Client OS    : Windows
  Client Type  : AnyConnect
  Client Ver   : 3.1.05050
```

```
IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 64251                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : 3DES                   Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86241 Seconds
  PRF          : SHA1                   D/H Group    : 2
  Filter Name  : mixed1
  Client OS    : Windows

IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 75.2.1.23/255.255.255.255/47/0
  Remote Addr  : 75.2.1.60/255.255.255.255/47/0
  Encryption   : 3DES                   Hashing      : SHA1
  Encapsulation: Transport, GRE
  Rekey Int (T): 28400 Seconds          Rekey Left(T): 28241 Seconds
  Idle Time Out: 400 Minutes            Idle TO Left : 400 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 21326
  Pkts Tx      : 0                      Pkts Rx      : 239

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 165 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

Output from **show vpn-sessiondb detail anyconnect** showing a DTLS tunnel.

```
...
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10280                  Bytes Rx     : 3819
Pkts Tx      : 8                      Pkts Rx      : 45
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : DefaultWEBVPNGroup
Login Time   : 09:42:39 UTC Tue Dec 5 2017
Duration     : 0h:00m:07s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 00000000000010005a266a0f
Security Grp : none
...
DTLS-Tunnel:
  Tunnel ID    : 1.3
  Assigned IP  : 95.0.225.240           Public IP    : 85.0.224.13
  Encryption   : AES256                 Hashing      : SHA1
  Ciphersuite  : AES256-SHA
  Encapsulation: DTLSv1.2             UDP Src Port : 51008
  UDP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.x
```

次に、**show vpn-sessiondb ra-ikev2-ipsec** コマンドの出力例を示します。

```
ciscoasa(config)# show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username     : IKEV2TG                Index        : 1
Assigned IP  : 95.0.225.200           Public IP    : 85.0.224.12
Protocol     : IKEv2 IPsec
License      : AnyConnect Essentials
Encryption   : IKEv2: (1)3DES  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 17844
Pkts Tx      : 0                      Pkts Rx      : 230
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG    Tunnel Group : IKEV2TG
Login Time   : 11:39:54 UTC Tue May 6 2014
Duration     : 0h:03m:17s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none

IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

次に、**show vpn-sessiondb license-summary** コマンドの出力例を示します。

```
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                  Status : Capacity : Installed :  Limit
                                 ----------------------------------------
AnyConnect Premium               : DISABLED :      250 :        10 :   NONE
AnyConnect Essentials            :  ENABLED :      250 :       250 :   NONE
Other VPN (Available by Default) :  ENABLED :      250 :       250 :   NONE
Shared License Server            : DISABLED
Shared License Participant       : DISABLED
AnyConnect for Mobile            : DISABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     : DISABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   : DISABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
----------------------------------------------------------------------------

----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
                        Local : Shared :   All  :   Peak :  Eff.  :
                       In Use : In Use : In Use : In Use :  Limit : Usage
                      ---------------------------------------------------
AnyConnect Essentials  :      1 :      0 :      1 :      1 :    250 :    0%
  AnyConnect Client    :                :      0 :      0          :    0%
    AnyConnect Mobile  :                :      0 :      0          :    0%
  Generic IKEv2 Client :                :      1 :      1          :    0%
Other VPN              :                :      0 :      0 :    250 :    0%
  Cisco VPN Client     :                :      0 :      0          :    0%

----------------------------------------------------------------------------
Shared License Network Summary
----------------------------------------------------------------------------
AnyConnect Premium
  Total shared licenses in network                                 : 500
```

```
  Shared licenses held by this participant                          :  0
  Shared licenses held by all participants in the network           :  0
-------------------------------------------------------------------------------
```

例に示すとおり、**show vpn-sessiondb** コマンドの応答に表示されるフィールドは、入力するキーワードによって異なります。これらのフィールドは、表 14-2 に説明されています。

表 14-2　show vpn-sessiondb コマンドのフィールド

フィールド	説明
Auth Mode	このセッションを認証するためのプロトコルまたはモード。
Bytes Rx	ASA がリモートのピアまたはクライアントから受信した合計バイト数。
Bytes Tx	ASA がリモートのピアまたはクライアントに送信した合計バイト数。
クライアント タイプ	リモート ピア上で実行されるクライアント ソフトウェア（利用できる場合）。
Client Ver	リモート ピア上で実行されるクライアント ソフトウェアのバージョン。
Connection	接続名またはプライベート IP アドレス。
D/H Group	Diffie-Hellman グループ。IPsec SA 暗号キーを生成するためのアルゴリズムおよびキー サイズ。
持続時間	セッションのログイン時刻から直前の画面リフレッシュまでの経過時間（HH:MM:SS）。
EAPoUDP Session Age	正常に完了した直前のポスチャ確認からの経過秒数。
カプセル化	IPsec ESP（暗号ペイロード プロトコル）の暗号化と認証（つまり、ESP を適用した元の IP パケットの一部）を適用するためのモード。
暗号化	このセッションが使用しているデータ暗号化アルゴリズム（ある場合）。
EoU Age (T)	EAPoUDP セッションの経過時間。正常に完了した直前のポスチャ確認からの経過秒数。
Filter Name	セッション情報の表示を制限するよう指定されたユーザ名。
ハッシュ	パケットのハッシュを生成するためのアルゴリズム。IPsec データ認証に使用されます。
Hold Left (T)	Hold-Off Time Remaining。直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
Hold-Off Time Remaining	直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
IKE Neg Mode	キー情報を交換し、SA を設定するための IKE（IPsec フェーズ 1）モード（アグレッシブまたはメイン）。
IKE Sessions	IKE（IPsec フェーズ 1）セッションの数で、通常は 1。これらのセッションにより、IPsec トラフィックのトンネルが確立されます。
索引	このレコードの固有識別情報。
IP Addr	このセッションのリモート クライアントに割り当てられたプライベート IP アドレス。このアドレスは、「内部」または「仮想」IP アドレスとも呼ばれています。このアドレスを使用すると、クライアントはプライベート ネットワーク内のホストと見なされます。

表 14-2　show vpn-sessiondb コマンドのフィールド(続き)

フィールド	説明
IPsec Sessions	IPsec(フェーズ 2)セッション(トンネル経由のデータ トラフィック セッション)の数。各 IPsec リモート アクセス セッションには、2 つの IPsec セッションがあります。1 つはトンネル エンドポイントで構成されるセッション、もう 1 つはトンネル経由で到達可能なプライベート ネットワークで構成されるセッションです。
ライセンス情報	共有 SSL VPN ライセンスに関する情報を表示します。
Local IP Addr	トンネルのローカル エンドポイント(ASA上のインターフェイス)に割り当てられた IP アドレス。
Login Time	セッションにログインした日時(MMM DD HH:MM:SS)。時刻は 24 時間表記で表示されます。
NAC Result	ネットワーク アドミッション コントロール ポスチャ検証の状態。次のいずれかを指定できます。 • [Accepted]:ACS は正常にリモート ホストのポスチャを検証しました。 • [Rejected]:ACS はリモート ホストのポスチャの検証に失敗しました。 • [Exempted]:ASA に設定されたポスチャ検証免除リストに従って、リモート ホストはポスチャ検証を免除されました。 • [Non-Responsive]:リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。 • [Hold-off]:ポスチャ検証に成功した後、ASA とリモート ホストの EAPoUDP 通信が途絶えました。 • [N/A]:VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。 • [Unknown]:ポスチャ検証が進行中です。
NAC Sessions	ネットワーク アドミッション コントロール(EAPoUDP)セッションの数。
Packets Rx	ASA がリモート ピアから受信したパケット数。
Packets Tx	ASA がリモート ピアに送信したパケット数。
PFS Group	完全転送秘密グループ番号。
Posture Token	Access Control Server 上で設定可能な情報テキスト ストリング。ACS は情報提供のために ASA にポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
Protocol	セッションが使用しているプロトコル。
Public IP	クライアントに割り当てられた、公開されているルーティング可能な IP アドレス。

表 14-2　show vpn-sessiondb コマンドのフィールド(続き)

フィールド	説明
リダイレクト URL	ポスチャ検証またはクライアントレス認証に続いて、ACS はセッションのアクセス ポリシーを ASA にダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。ASA は、リモート ホストのすべての HTTP(ポート 80)要求および HTTPS(ポート 443)要求を Redirect URL(存在する場合)にリダイレクトします。アクセス ポリシーに Redirect URL が含まれていない場合、ASA はリモート ホストからの HTTP 要求および HTTPS 要求をリダイレクトしません。 Redirect URL は、IPsec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。
Rekey Int(T または D)	IPsec(IKE)SA 暗号キーの有効期限。T 値は時間でのライフタイム、D 値は送信済みデータでのライフタイムです。リモート アクセス VPN では T 値のみが表示されます。
Rekey Left(T または D)	IPsec(IKE)SA 暗号キーの残りのライフタイム。T 値は時間でのライフタイム、D 値は送信済みデータでのライフタイムです。リモート アクセス VPN では T 値のみが表示されます。
Rekey Time Interval	IPsec(IKE)SA 暗号キーの有効期限。
Remote IP Addr	トンネルのリモート エンドポイント(リモート ピア上のインターフェイス)に割り当てられた IP アドレス。
Reval Int (T)	Revalidation Time Interval。正常に完了した各ポスチャ確認間に、設ける必要のある間隔(秒単位)。
Reval Left (T)	Time Until Next Revalidation。直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Revalidation Time Interval	正常に完了した各ポスチャ確認間に、設ける必要のある間隔(秒単位)。
Session ID	セッション コンポーネント(サブセッション)の ID。各 SA には独自の ID があります。
Session Type	セッションのタイプ(LAN-to-LAN または Remote)。
SQ Int (T)	Status Query Time Interval。正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、ASA がリモート ホストに発行する要求です。
Status Query Time Interval	正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、ASA がリモート ホストに発行する要求です。
Time Until Next Revalidation	直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。

表 14-2　show vpn-sessiondb コマンドのフィールド(続き)

フィールド	説明
Tunnel Group	属性値を求めるために、このトンネルが参照するトンネル グループの名前。
UDP Dst Port または UDP Destination Port	リモート ピアが使用する UDP のポート番号。
UDP Src Port または UDP Source Port	ASA が使用する UDP のポート番号。
Username	セッションを確立したユーザのログイン名。
VLAN	このセッションに割り当てられた出力 VLAN インターフェイス。ASA は、すべてのトラフィックをこの VLAN に転送します。次のいずれかの要素で値を指定します。 • グループ ポリシー • 継承されたグループ ポリシー

関連コマンド

コマンド	説明
show running-configuration vpn-sessiondb	VPN セッション データベースの実行コンフィギュレーション(max-other-vpn-limit、max-anyconnect-premium-or-essentials-limit)を表示します。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。

show vpn-sessiondb ratio

現在のセッションについて、プロトコルごと、または暗号化アルゴリズムごとの比率をパーセンテージで表示するには、特権 EXEC モードで **show vpn-sessiondb ratio** コマンドを使用します。

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

構文の説明

暗号化	表示する暗号化プロトコルを指定します。フェーズ 2 暗号化に関して指定します。暗号化アルゴリズムには次の種類があります。	
	aes128	des
	aes192	3des
	aes256	rc4
filter *groupname*	出力をフィルタリングして、指定するトンネル グループについてのみセッションの比率を表示します。	
protocol	表示するプロトコルを指定します。プロトコルには次の種類があります。	
	IKEv1	L2TPOverIPsecOverNatT
	IKEv2	クライアントレス
	IPSec	ポート転送
	IPsecLAN2LAN	IMAP4S
	IPsecLAN2LANOverNatT	POP3S
	IPsecOverNatT	SMTPS
	IPsecOverTCP	AnyConnect-Parent
	IPsecOverUDP	SSL トンネル
	L2TPOverIPsec	DTLS トンネル

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	出力が拡張され、IKEv2 が含まれるようになりました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、引数として **encryption** を指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
ciscoasa# show vpn-sessiondb ratio encryption
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions       Percent
none                     0               0%
DES                      1              20%
3DES                     0               0%
AES128                   4        80%
AES192                   0               0%
AES256                   0               0%
```

次に、引数として **protocol** を指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
ciscoasa# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions       Percent
IKE                      0               0%
IPsec                    1              20%
IPsecLAN2LAN             0               0%
IPsecLAN2LANOverNatT     0               0%
IPsecOverNatT            0               0%
IPsecOverTCP             1 20%
IPsecOverUDP             0               0%
L2TP                     0               0%
L2TPOverIPsec            0               0%
L2TPOverIPsecOverNatT    0               0%
PPPoE                    0               0%
vpnLoadBalanceMgmt       0               0%
userHTTPS                0               0%
IMAP4S                   3 30%
POP3S                    0               0%
SMTPS                    3 30%
```

関連コマンドshow

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb summary	セッションの要約を表示します。現在のセッションの合計数、各タイプの現在のセッション数、ピーク時の数および累積合計数、最大同時セッション数を含んでいます。

show vpn-sessiondb summary

IPsec、Cisco AnyConnect、および NAC の各セッションの数を表示するには、特権 EXEC モードで **show vpn-sessiondb summary** コマンドを使用します。

show vpn-sessiondb summary

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(7)	このコマンドが追加されました。
8.0(2)	VLAN Mapping Sessions テーブルが追加されました。
8.0(5)	active（アクティブ）、cumulative（累積）、peak concurrent（ピーク時の同時発生）、および inactive（非アクティブ）に関する新しい出力が追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、1 つの IPsec IKEv1 および 1 つのクライアントレス セッションを指定した **show vpn-sessiondb summary** コマンドの出力例を示します。

（注） スタンバイ状態のデバイスでは、アクティブなセッションと非アクティブなセッションが区別されません。

```
ciscoasa# show vpn-sessiondb summary

VPN Session Summary
Sessions:
                        Active :Cumulative :Peak Concurrent :Inactive :
    Clientless VPN            :       1:         2:             1
    Browser                   :       1:         2:             1
    IKEv1 IPsec/L2TP IPsec0   :       1:         1:             1

Total Active and Inactive: 2      Total Cumulative: 3
Device Total VPN Capacity: 10000
Device Load            : 0%
```

```
License Information:
    Shared VPN License Information:
        SSL VPN                         : 12000
            Allocated to this device    :    0
            Allocated to network        :    0
            Device limit                : 750

IPsec   :   750     Configured :750     Active : 0      Load : 0%
SSL VPN :   750     Configured :750     Active : 0      Load : 0%
                        Active : Cumulative : Peak Concurrent
SSL VPN         :           0 :         1 :             1
Totals          :           0 :         1 :

Active NAC Sessions:
  Accepted                : 0
  Rejected                : 0
  Exempted                : 0
  Non-responsive          : 0
Hold-off                : 0
  N/A                     : 0

Active VLAN Mapping Sessions:
  Static                  : 0
  Auth                    : 0
  Access                  : 0
  Guest                   : 0
  Quarantine              : 0
  N/A                     : 0

ciscoasa#
```

SSL 出力を使用して、ライセンス数に関する物理デバイス リソースを特定できます。単一のユーザ セッションがライセンスを占有し、かつ複数のトンネルを使用することがあります。たとえば、DTLS を使用する AnyConnect ユーザは、通常、それに関連する親セッション、SSL トンネル、および DTLS トンネルを使用します。

(注) 親セッションは、クライアントがアクティブに接続されていない場合を示します。暗号化トンネルは表しません。クライアントがシャットダウンしたかスリープ中である場合、IPsec、IKE、TLS、および DLTLS トンネルは閉じられますが、アイドル時間または最大接続時間の制限に到達するまで親セッションが維持されます。これにより、ユーザは再認証しないで再接続できます。

この例では、ログインしているユーザが 1 人の場合でも、デバイスに割り当てられている 3 つのトンネルが表示されます。IPsec LAN-to-LAN トンネルは 1 セッションとしてカウントされ、トンネルを通じて多くのホスト間接続を可能にします。IPsec リモート アクセス セッションは、1 つのユーザ接続をサポートする 1 リモート アクセス トンネルです。

出力から、アクティブなセッションを確認できます。セッションに関連付けられた、基本となるトンネルがない場合、ステータスは *再開待ち* モードになります(セッション出力にクライアントレスとして表示されます)。このモードは、ヘッドエンド デバイスからのデッドピア検出が開始され、ヘッドエンド デバイスがクライアントと通信できないことを意味します。この状態が発生した場合は、ユーザがネットワークをローミングしたり、スリープにしたり、セッションを再開したりすることができるように、セッションを保持できます。これらのセッションは、アクティブに接続されたセッション(ライセンスの観点から)にカウントされ、ユーザのアイドル タイムアウト、ユーザのログアウト、または元のセッション再開でクリアされます。

SSL VPN With Client の Active 列には、データを送信しているアクティブな接続の数が表示されます。SSL VPN With Client の Cumulative 列には、確立されているアクティブなセッションの数が表示されます。この数には非アクティブなセッションの数が含まれており、新しいセッションが追加された場合にのみ値が増加します。SSL VPN With Client の Peak Concurrent 列には、データを送信中で、同時にアクティブなセッションのピーク数が表示されます。SSL VPN、With Client の Inactive 列には、AnyConnect クライアントが切断されている期間が表示されます。この非アクティビティ タイムアウト値を使用して、ライセンスをいつ期限切れにするかを決定できます。ASA は、再接続が可能かどうかを決定できます。これらのセッションは、アクティブな SSL トンネルが関連付けられていない AnyConnect セッションです。

表 14-3 に、Active Sessions テーブルと Session Information テーブルにあるフィールドの説明を示します。

表 14-3　show vpn-sessiondb summary コマンド:Active Sessions および Session Information のフィールド

フィールド	説明
Concurrent Limit	この ASA 上で許可された、同時にアクティブなセッションの最大数。
Cumulative Sessions	ASA が最後に起動またはリセットされたとき以降のすべてのタイプのセッション数。
LAN-to-LAN	現在アクティブな IPsec LAN-to-LAN セッションの数。
Peak Concurrent	ASA が最後に起動またはリセットされたとき以降に同時に有効（アクティブおよび非アクティブ）であった、すべてのタイプのセッションの最大数。
Percent Session Load	使用中の vpn セッション割り当てのパーセンテージ。この値は、Total Active Sessions を利用可能なセッションの最大数で除算した値に等しく、パーセンテージで表示されます。利用可能なセッションの最大数は、次のいずれかの値です。 • ライセンスのある IPsec セッションおよび SSL VPN セッションの最大数 • **vpn-sessiondb ?**（設定された最大セッション数） • **max-anyconnect-premium-or-essentials-limit**（AnyConnect Premium または AnyConnect Essentials セッションの最大制限） • **max-other-vpn-limit**（その他の VPN セッションの最大制限）
Remote Access	ra-ikev1-ipsec：現在アクティブな IKEv1 IPsec リモート アクセス ユーザ、L2TP over IPsec、および IPsec through NAT セッションの数。
Total Active Sessions	現在アクティブなすべてのタイプのセッションの数。

Active NAC Sessions テーブルには、ポスチャ検証の対象であるリモート ピアに関する一般的な統計情報が表示されます。

Cumulative NAC Sessions テーブルには、ポスチャ検証の対象である、または以前から対象であったリモート ピアに関する一般的な統計情報が表示されます。

表 14-2 に、Active NAC Sessions テーブルおよび Total Cumulative NAC Sessions テーブルにあるフィールドの説明を示します。

表 14-4 show vpn-sessiondb summary コマンド:Active NAC Sessions および Total Cumulative NAC Sessions のフィールド

フィールド	説明
Accepted	ポスチャ検証が成功し、Access Control Server によってアクセス ポリシーが付与されたピアの数。
Exempted	ASA 上に設定されたポスチャ検証免除リストのエントリに一致しているため、ポスチャ検証の対象とならないピアの数。
Hold-off	ASA がポスチャ検証に成功した後、EAPoUDP 通信が途絶えたピアの数。このタイプのイベントが発生してから各ピアに対して次にポスチャ検証が試行されるまでの遅延は、NAC Hold Timer 属性（[Configuration] > [VPN] > [NAC]）によって決まります。
該当なし	VPN NAC グループ ポリシーに従って NAC がディセーブルになっているピアの数。
Non-responsive	ポスチャ検証のための拡張認証プロトコル（EAP）over UDP 要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。ASA のコンフィギュレーションがクライアントレス ホストをサポートする場合、Access Control Server は、クライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアの ASA にダウンロードします。クライアントレス ホストをサポートしない場合、ASA は NAC デフォルト ポリシーを割り当てます。
Rejected	ポスチャ検証に失敗したか、または Access Control Server によってアクセス ポリシーが付与されなかったピアの数。

Active VLAN Mapping Sessions テーブルには、ポスチャ検証の対象であるリモート ピアに関する一般的な統計情報が表示されます。

Cumulative VLAN Mapping Sessions テーブルには、ポスチャ検証の対象である、または以前から対象であったリモート ピアに関する一般的な統計情報が表示されます。

表 14-5 に、Active VLAN Mapping Sessions テーブルおよび Cumulative VLAN Mapping Sessions テーブルにあるフィールドの説明を示します。

表 14-5 show vpn-sessiondb summary コマンド:Active VLAN Mapping Sessions および Cumulative Active VLAN Mapping Sessions のフィールド

フィールド	説明
アクセス	将来的な使用のために予約されています。
認証	将来的な使用のために予約されています。
Guest	将来的な使用のために予約されています。
該当なし	将来的な使用のために予約されています。
Quarantine	将来的な使用のために予約されています。
スタティック	このフィールドには、事前設定された VLAN に割り当てられている VPN セッションの数が表示されます。

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。

show wccp

Web Cache Communication Protocol（WCCP）に関連するグローバル統計情報を表示するには、特権 EXEC モードで **show wccp** コマンドを使用します。

show wccp {**web-cache** | *service-number*}[*detail* | *view*]

構文の説明

detail	（任意）ルータおよびすべての Web キャッシュに関する情報を表示します。
service-number	（任意）キャッシュが制御する Web キャッシュ サービス グループの ID 番号。指定できる番号の範囲は 0 ～ 256 です。Cisco Cache Engine を使用する Web キャッシュの場合、逆プロキシ サービスの値には 99 を指定します。
view	（任意）特定のサービス グループの他のメンバーが検出されたかどうかを表示します。
web-cache	Web キャッシュ サービスの統計情報を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、WCCP 情報を表示する例を示します。

```
ciscoasa(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0

    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
```

```
        Total Packets Unassigned:           0
        Group access-list:                  foobar
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
wccp	サービス グループを使用して、WCCP のサポートをイネーブルにします。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

show webvpn anyconnect

ASA にインストールされ、キャッシュ メモリにロードされる SSL VPN クライアント イメージに関する情報を表示したり、ファイルをテストして有効なクライアント イメージかどうかを確認したりするには、特権 EXEC モードで **show webvpn anyconnect** コマンドを使用します。

show webvpn anyconnect [**image** *filename*]

構文の説明

image *filename*	SSL VPN クライアント イメージ ファイルとしてテストするファイルの名前を指定します。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.4(1)	コマンドの **show webvpn anyconnect** 形式が **show webvpn svc** と置き換わりました。

使用上のガイドライン

キャッシュ メモリにロードされ、リモート PC にダウンロード可能な SSL VPN クライアント イメージに関する情報を表示するには、**show webvpn anyconnect** コマンドを使用します。ファイルをテストして有効なイメージかどうかを確認するには、**image** *filename* のキーワードと引数を使用します。ファイルが有効なイメージではない場合、次のメッセージが表示されます。

```
ERROR: This is not a valid SSL VPN Client image file.
```

例

次に、現在インストールされているイメージに対する **show webvpn anyconnect** コマンドの出力例を示します。

```
ciscoasa# show webvpn anyconnect
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

```
2. window2.pkg 2
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

次に、有効なイメージに対する **show webvpn anyconnect image** *filename* コマンドの出力例を示します。

```
ciscoasa(config-webvpn)# show webvpn anyconnect image sslclient-win-1.0.2.127.pkg

This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

関連コマンド

コマンド	説明
anyconnect enable	ASA で SSL VPN クライアントをリモート PC にダウンロードできるようにします。
anyconnect image	セキュリティ アプライアンスがフラッシュ メモリからキャッシュ メモリに SSL VPN クライアント ファイルをロードするようにします。クライアント イメージをオペレーティング システムと照合するときに、セキュリティ アプライアンスがクライアント イメージの各部分をリモート PC にダウンロードする順序を指定します。
vpn-tunnel-protocol	SSL VPN クライアントが使用する SSL を含め、リモート VPN ユーザの特定の VPN トンネル プロトコルをイネーブルにします。

show webvpn csd（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

CSD がイネーブルかどうかを特定したり、実行コンフィギュレーションの CSD バージョンを表示したり、ホスト スキャン パッケージを提供しているイメージを特定したり、ファイルをテストして有効な CSD 配布パッケージかどうかを確認したりするには、特権 EXEC モードで **show webvpn csd** コマンドを使用します。

show webvpn csd [**image** *filename*]

構文の説明

filename	CSD 配布パッケージとしての有効性をテストするファイルの名前を指定します。**csd_n.n.n-k9.pkg** の形式にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。**show webvpn hostscan** によって置き換えられました。

例

CSD の動作ステータスを確認するには、**show webvpn csd** コマンドを使用します。CLI は、CSD がインストールされ、イネーブルになっているかどうか、ホスト スキャン パッケージがインストールされ、イネーブルになっているかどうかを示すメッセージで応答します。また、CSD パッケージとホスト スキャン パッケージの両方がインストールされている場合は、どちらのイメージがホスト スキャン パッケージを提供しているかも、メッセージに示されます。

```
ciscoasa# show webvpn csd
```

受信する可能性があるメッセージは、次のとおりです。

- `Secure Desktop is not installed`
  `Hostscan is not installed`

- `Secure Desktop version n.n.n.n is currently installed but not enabled`

  `Standalone Hostscan package is not installed (Hostscan is currently installed via the CSD package but not enabled)`

- `Secure Desktop version n.n.n.n is currently installed and enabled`

  `Standalone Hostscan package is not installed (Hostscan is currently installed and enabled via the CSD package)`

  「`Secure Desktop version n.n.n.n is currently installed ...`」というメッセージは、イメージが ASA にロードされ、実行コンフィギュレーションにあることを意味します。イメージは、**enabled** または **not enabled** のいずれかになります。webvpn コンフィギュレーション モードを開始し、**csd enable** コマンドを入力することで、CSD をイネーブルにすることができます。

  メッセージ「`(Hostscan is currently installed and enabled via the CSD package)`」は、CSD パッケージとともに提供されたホスト スキャン パッケージが使用中のホスト スキャン パッケージであることを意味します。

- `Secure Desktop version n.n.n.n is currently installed and enabled`

  `Hostscan version n.n.n.n is currently installed and enabled`

  「`Secure Desktop version n.n.n.n is currently installed and enabled Hostscan version n.n.n.n is currently installed and enabled`」というメッセージは、CSD と、スタンドアロン パッケージまたは AnyConnect イメージの一部のいずれかとして配布されたホスト スキャン パッケージの両方がインストールされていることを意味します。ホスト スキャンがイネーブルで、ホスト スキャンを使用する CSD および AnyConnect イメージの両方、またはスタンドアロンのホスト スキャン パッケージがインストールされ、イネーブルになっている場合、スタンドアロン パッケージとして、または AnyConnect イメージの一部として提供されるホスト スキャン パッケージは、CSD パッケージに付属しているものよりも優先されます。

- `Secure Desktop version n.n.n.n is currently installed but not enabled`

  `Hostscan version n.n.n.n is currently installed but not enabled`

ファイルをテストして、CSD 配布パッケージが有効かどうかを確認するには、**show webvpn csd image *filename*** コマンドを使用します。

ciscoasa# **`show webvpn csd image csd_n.n.n-k9.pkg`**

このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- `ERROR: This is not a valid Secure Desktop image file.`

  ファイル名は必ず **csd_n.n.n_k9.pkg** の形式にしてください。CSD パッケージがこの命名規則に従っていない場合、次の Web サイトから取得したファイルに置き換えます。

  http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

  次に、**show webvpn csd image** コマンドを再入力します。イメージが有効な場合は、webvpn コンフィギュレーション モードで **csd image** コマンドおよび **csd enable** コマンドを使用し、CSD をインストールしてイネーブルにします。

- `This is a valid Cisco Secure Desktop image:`

  `Version  : 3.6.172.0`

  `Hostscan Version  : 3.6.172.0`

  `Built on : Wed Feb 23 15:46:44 MST 2011`

  ファイルが有効な場合は、CLI にバージョンおよび日付スタンプが表示されます。

関連コマンド

コマンド	説明
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。
csd image	コマンドに指定された CSD イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。

show webvpn group-alias

特定のトンネル グループまたはすべてのトンネル グループのエイリアスを表示するには、特権 EXEC モードで **group-alias** コマンドを使用します。

show webvpn group-alias [*tunnel-group*]

構文の説明

tunnel-group	（任意）グループ エイリアスを表示する特定のトンネル グループを指定します。

デフォルト

トンネル グループ名が入力されなかった場合は、すべてのトンネル グループのすべてのエイリアスが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1	このコマンドが追加されました。

使用上のガイドライン

show webvpn group-alias コマンドを入力する場合は、WebVPN が実行されている必要があります。

各トンネル グループには複数のエイリアスがあることも、エイリアスがまったくないこともあります。

例

次に、トンネル グループ「devtest」のエイリアスを表示する **show webvpn group-alias** コマンドと、このコマンドの出力例を示します。

```
ciscoasa# show webvpn group-alias devtest
QA
Fra-QA
```

関連コマンド

コマンド	説明
group-alias	グループに対して 1 つ以上の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

show webvpn group-url

特定のトンネル グループまたはすべてのトンネル グループの URL を表示するには、特権 EXEC モードで **group-url** コマンドを使用します。

show webvpn group-url [*tunnel-group*]

構文の説明

tunnel-group	（任意）URL を表示する特定のトンネル グループを指定します。

デフォルト

トンネル グループ名が入力されなかった場合は、すべてのトンネル グループのすべての URL が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

show webvpn group-url コマンドを入力する場合は、WebVPN が実行されている必要があります。各グループには複数の URL があることも、URL がまったくないこともあります。

例

次に、トンネル グループ「frn-eng1」の URL を表示する **show webvpn group-url** コマンドと、このコマンドの出力例を示します。

```
ciscoasa# show webvpn group-url
http://www.cisco.com
https://fra1.example.com
https://fra2.example.com
```

関連コマンド

コマンド	説明
group-url	グループに対して 1 つ以上の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

show webvpn hostscan

ホストスキャンが有効かどうかを特定したり、実行コンフィギュレーションのホストスキャン バージョンを表示したり、ホストスキャン パッケージを提供しているイメージを特定したり、ファイルをテストして有効なホストスキャン配布パッケージかどうかを確認したりするには、特権 EXEC モードで **show webvpn hostscan** コマンドを使用します。

show webvpn hostscan [**image** *filename*]

構文の説明

filename	ホストスキャン配布パッケージとしての有効性をテストするファイルの名前を指定します。**hostscan_4.1.04011-k9.pkg** の形式にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

例

ホストスキャンの動作ステータスを確認するには、**show webvpn hostscan** コマンドを使用します。CLI は、ホストスキャンがインストールされているかどうか、それが有効になっているかどうか、どのイメージがホストスキャン パッケージを提供しているかを示すメッセージで応答します。

```
ciscoasa# show webvpn hostscan
```

受信する可能性があるメッセージは、次のとおりです。

- `Hostscan is not installed`
- `Hostscan n.n.n is currently installed and enabled`

  「`Hostscan version n.n.n is currently installed ...`」というメッセージは、イメージが ASA にロードされ、実行コンフィギュレーションに含まれていることを意味します。イメージは、**enabled** または **not enabled** のいずれかになります。webvpn コンフィギュレーション モードを開始し、**hostscan enable** コマンドを入力することで、CSD を有効にすることができます。

- `Hostscan version n.n.n is currently installed but not enabled`

  ファイルをテストして、ホストスキャン配布パッケージが有効かどうかを確認するには、**show webvpn hostscan image** ***filename*** コマンドを使用します。

  ciscoasa# **show webvpn hostscan image hostscan_4.1.04011-k9.pkg**

  このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

  - `ERROR: This is not a valid Hostscan image file.`

    ファイル名は必ず **hostscan_n.n.n-k9.pkg** の形式にしてください。ホストスキャン パッケージにこの命名規則が使用されていない場合は、使用している AnyConnect のバージョンに適したファイルをシスコ ダウンロード サイトから取得し、それと置き換えます。

    その後、**show webvpn hostscan image** コマンドを再度入力します。イメージが有効な場合は、webvpn コンフィギュレーション モードで **hostscan image** コマンドと **hostscan enable** コマンドを使用して、ホストスキャンをインストールして有効にします。

  - `This is a valid Hostscan image:`
    `Version : 4.1.4011`
    `Built on : Mon July 27 15:46:44 MST 2015`

  ファイルが有効な場合は、CLI にバージョンおよび日付スタンプが表示されます。

関連コマンド

コマンド	説明
hostscan enable	管理およびリモート ユーザ アクセスのホストスキャンをイネーブルにします。
hostscan image	コマンドに指定されたホストスキャン イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。

show webvpn kcd

ASA のドメイン コントローラの情報およびドメイン参加ステータスを表示するには、webvpn コンフィギュレーション モードで **show webvpn kcd** コマンドを使用します。

show webvpn kcd

構文の説明

なし。

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

webvpn コンフィギュレーション モードで **show webvpn kcd** コマンドを使用すると、ASA のドメイン コントローラの情報およびドメイン参加ステータスが表示されます。

例

次に、**show webvpn kcd** コマンドで注意する必要がある重要な詳細と、ステータス メッセージの解釈の例を示します。

次に、登録が進行中で終了していない例を示します。

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNAL
Domain Join: In-Progress
```

次に、登録が成功し、ASA がドメインに参加している例を示します。

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNAL
Domain Join: Complete
```

関連コマンド

コマンド	説明
clear aaa kerberos	ASA でキャッシュされたすべての Kerberos チケットをクリアします。
kcd-server	ASA は Active Directory ドメインに参加できます。
show aaa kerberos	ASA 上のキャッシュされたすべての Kerberos チケットを表示します。

show webvpn sso-server（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

WebVPN シングル サインオン サーバに関する運用統計情報を表示するには、特権 EXEC モードで **show webvpn sso-server** コマンドを使用します。

show webvpn sso-server [*name*]

構文の説明

name	（任意）SSO サーバの名前を指定します。サーバ名の長さは 4 ～ 31 文字にする必要があります。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
config-webvpn-sso-saml	• 対応	—	• 対応	—	—
config-webvpn-sso-siteminder	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**show webvpn sso-server** コマンドは、セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。

SSO サーバ名引数が入力されていない場合は、すべての SSO サーバの統計情報が表示されます。

例

次に、特権 EXEC モードでコマンドを入力し、タイプが SiteMinder、名前が example である SSO サーバの統計情報を表示する例を示します。

```
ciscoasa# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
ciscoasa#
```

次に、SSO サーバ名を指定しないでコマンドを発行し、ASA に設定されているすべての SSO サーバの統計情報が表示される例を示します。

```
ciscoasa#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
max-retry-attempts	ASA が、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder-type SSO サーバへの認証要求の暗号化に使用される秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

show xlate

NAT セッション（xlates）の情報を表示するには、特権 EXEC モードで **show xlate** コマンドを使用します。

show xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]] [**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**type** *type*]

show xlate count

構文の説明

count	変換数を表示します。
global *ip1*[**-***ip2*]	（任意）アクティブな変換をマッピングされた IP アドレスまたはアドレスの範囲別に表示します。
gport *port1*[*-port2*]	（任意）アクティブな変換をマッピングされたポートまたはポートの範囲別に表示します。
interface *if_name*	（任意）アクティブな変換をインターフェイス別に表示します。
local *ip1*[**-***ip2*]	（任意）アクティブな変換を実際の IP アドレスまたはアドレスの範囲別に表示します。
lport *port1*[*-port2*]	（任意）アクティブな変換を実際のポートまたはポートの範囲別に表示します。
netmask *mask*	（任意）マッピングされた、または実際の IP アドレスを限定するネットワーク マスクを指定します。
type *type*	（任意）アクティブな変換をタイプ別に表示します。次のタイプを 1 つ以上入力できます。 • **静的** • **portmap** • **dynamic** • **twice-nat** 複数のタイプを指定する場合は、タイプをカンマで区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドは、新しい NAT 実装をサポートするように変更されました。
8.4(3)	拡張 PAT の使用を表示するために **e** フラグが追加されました。また、xlate が拡張された宛先アドレスが表示されます。
9.0(1)	このコマンドは、IPv6 をサポートするように変更されました。

使用上のガイドライン

show xlate コマンドは、変換スロットの内容を表示します。

vpnclient コンフィギュレーションがイネーブルで、内部ホストが DNS 要求を送信している場合に **show xlate** コマンドを実行すると、1 つのスタティック変換に対応する複数の xlate が表示されることがあります。

ASA クラスタリング環境では、PAT セッションを処理するために、最大 3 つの xlate が、クラスタ内の異なるノードに複製される可能性があります。1 つの xlate は、接続を所有するユニットで作成されます。1 つの xlate は、PAT アドレスをバックアップするために別のユニットで作成されます。最後の 1 つの xlate は、フローを複製するディレクタにあります。バックアップとディレクタが同じユニットである場合、3 つではなく 2 つの xlate が作成されることがあります。

宛先変換を指定せずに 2 回 NAT ルールを作成すると、システムはそれをあらゆるアドレスに対する静的変換と解釈します。そのため、NAT テーブルには、0.0.0.0/0 から 0.0.0.0/0 への変換が含まれます。このルールは、2 度目の NAT ルールから暗黙的に示されます。

例

次に、**show xlate** コマンドの出力例を示します。

```
ciscoasa# show xlate
5 in use, 5 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
NAT from any:10.90.67.2 to any:10.9.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.90.67.2 to any:10.86.94.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.9.0.9, 10.9.0.10/31, 10.9.0.12/30,
    10.9.0.16/28, 10.9.0.32/29, 10.9.0.40/30,
    10.9.0.44/31 to any:0.0.0.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:14 timeout 0:00:00
```

次に、**e - extended** フラグと xlate が拡張されている宛先アドレスの使用を示す **show xlate** コマンドの出力例を示します。

```
ciscoasa# show xlate
1 in use, 1 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
ICMP PAT from inside:10.2.1.100/6000 to outside:172.16.2.200/6000(172.16.2.99)
    flags idle 0:00:06 timeout 0:00:30
TCP PAT from inside:10.2.1.99/5 to outside:172.16.2.200/5(172.16.2.90)
    flags idle 0:00:03 timeout 0:00:30
UDP PAT from inside:10.2.1.101/1025 to outside:172.16.2.200/1025(172.16.2.100)
    flags idle 0:00:10 timeout 0:00:30
```

次に、IPv4 から IPv6 への変換を示す **show xlate** コマンドの出力例を示します。

```
ciscoasa# show xlate
1 in use, 2 most used
NAT from outside:0.0.0.0/0 to in:2001::/96
flags sT idle 0:16:16 timeout 0:00:00
```

関連コマンド

コマンド	説明
clear xlate	現在の変換および接続情報をクリアします。
show conn	すべてのアクティブ接続を表示します。
show local-host	ローカル ホスト ネットワーク情報を表示します。
show uauth	現在認証済みのユーザを表示します。

show zone

ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示するには、特権 EXEC モードで **show zone** コマンドを使用します。

show zone [*name*]

構文の説明

name	（オプション）**zone** コマンドで設定されたゾーン名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

ゾーン設定を表示するには、**show running-config zone** コマンドを使用します。

例

show zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

関連コマンド

コマンド	説明
clear configure zone	ゾーンのコンフィギュレーションをクリアします。
clear conn zone	ゾーン接続をクリアします。
clear local-host zone	ゾーンのホストをクリアします。
show asp table routing	デバッグ目的で高速セキュリティ パス テーブルを表示し、各ルートに関連付けられたゾーンを表示します。
show asp table zone	デバッグ目的で高速セキュリティ パス テーブルを表示します。
show conn long	ゾーンの接続情報を表示します。
show local-host zone	ゾーン内のローカル ホストのネットワーク状態を表示します。
show nameif zone	インターフェイス名およびゾーン名を表示します。
show route zone	ゾーン インターフェイスのルートを表示します。
show running-config zone	ゾーンのコンフィギュレーションを表示します。
zone	トラフィック ゾーンを設定します。
zone-member	トラフィック ゾーンにインターフェイスを割り当てます。

shun コマンド～ sntp address コマンド

shun

攻撃元ホストからの接続をブロックするには、特権 EXEC モードで **shun** コマンドを使用します。shun をディセーブルにするには、このコマンドの **no** 形式を使用します。

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

構文の説明

dest_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先ポートを指定します。
dest_ip	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先アドレスを指定します。
protocol	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の IP プロトコル（UDP や TCP など）を指定します。デフォルトでは、プロトコルは 0（すべてのプロトコル）です。
source_ip	攻撃元ホストのアドレスを指定します。送信元 IP アドレスのみを指定した場合、このアドレスからの今後のすべての接続はドロップされます。現在の接続はそのまま維持されます。現在の接続をドロップし、かつ shun を適用するには、その接続についての追加パラメータを指定します。その送信元 IP アドレスからの今後のすべての接続には、宛先パラメータに関係なく、shun がそのまま維持されます。
source_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする、現在の接続の送信元ポートを指定します。
vlan_id	（任意）送信元ホストが配置されている VLAN ID を指定します。

デフォルト

デフォルトのプロトコルは 0（すべてのプロトコル）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

shun コマンドを使用すると、攻撃元ホストからの接続をブロックできます。送信元 IP アドレスからの今後のすべての接続は、手動または Cisco IPS センサーによってブロッキング機能が削除されるまで、ドロップされ、ログに記録されます。**shun** コマンドのブロッキング機能は、指定したホスト アドレスとの接続が現在アクティブかどうかに関係なく適用されます。

宛先アドレス、送信元ポート、宛先ポート、およびプロトコルを指定すると、一致する接続がドロップされ、かつ、その送信元 IP アドレスからの今後のすべての接続に shun が適用されます。この場合、これらの特定の接続パラメータと一致する接続だけでなく、今後のすべての接続が回避されます。

shun コマンドは、送信元 IP アドレスごとに 1 つのみ使用できます。

shun コマンドは攻撃をダイナミックにブロックするために使用されるため、ASA コンフィギュレーションには表示されません。

インターフェイス コンフィギュレーションが削除されると、そのインターフェイスに付加されているすべての shun も削除されます。新しいインターフェイスを追加するか、または同じインターフェイスを（同じ名前を使用して）置き換える場合、IPS センサーでそのインターフェイスをモニタするには、そのインターフェイスを IPS センサーに追加する必要があります。

例

次に、攻撃ホスト（10.1.1.27）が攻撃対象（10.2.2.89）に TCP で接続する例を示します。この接続は、ASA 接続テーブル内で次のように記載されています。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

次のオプションを使用して、**shun** コマンドを適用します。

```
ciscoasa# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

このコマンドにより、現在の接続は ASA 接続テーブルから削除され、10.1.1.27 からの今後のすべてのパケットは ASA を通過できなくなります。

関連コマンド

コマンド	説明
clear shun	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
show conn	すべてのアクティブな接続を表示します。
show shun	回避についての情報を表示します。

shutdown（ca サーバ）

ローカル認証局（CA）サーバをディセーブルにし、ユーザが登録インターフェイスにアクセスできないようにするには、CA サーバ コンフィギュレーション モードで **shutdown** コマンドを使用します。CA サーバをイネーブルにし、コンフィギュレーションをロックして変更できないようにし、登録インターフェイスにアクセスできるようにするには、このコマンドの **no** 形式を使用します。

[no] shutdown

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

最初は、CA サーバはデフォルトでシャットダウンされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CA サーバ モードのこのコマンドは、インターフェイス モードの **shutdown** コマンドと類似しています。セットアップ時に、ローカル CA サーバはデフォルトでシャットダウンされるため、**no shutdown** コマンドを使用してイネーブルにする必要があります。**no shutdown** コマンドを初めて使用するときは、CA サーバをイネーブルにし、CA サーバ証明書とキー ペアを生成します。

（注） **no shutdown** コマンドを発行することによって、CA コンフィギュレーションをロックして CA 証明書を生成した後は、CA コンフィギュレーションを変更できません。

no shutdown コマンドで CA サーバをイネーブルにして現在のコンフィギュレーションをロックするには、生成される CA 証明書とキー ペアが含まれる PKCS12 ファイルを符号化してアーカイブするために、7 文字のパスワードが必要です。このファイルは、以前に指定した **database path** コマンドで識別されるストレージに格納されます。

例

次に、ローカル CA サーバをディセーブルにし、登録インターフェイスにアクセスできないようにする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# shutdown
ciscoasa(config-ca-server)#
```

次に、ローカル CA サーバをイネーブルにし、登録インターフェイスにアクセスできるようにする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no shutdown
ciscoasa(config-ca-server)#

ciscoasa(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin. Please wait...

ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
show crypto ca server	CA コンフィギュレーションのステータスを表示します。

shutdown（インターフェイス）

インターフェイスをディセーブルにするには、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを使用します。インターフェイスをイネーブルにするには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

すべての物理インターフェイスは、デフォルトではシャットダウンされます。セキュリティ コンテキスト内の割り当て済みのインターフェイスは、コンフィギュレーション内でシャットダウンされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。

使用上のガイドライン

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス:ディセーブル。
- 冗長インターフェイス:イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス:イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

(注) このコマンドでは、ソフトウェア インターフェイスのみがディセーブルになります。物理リンクはアップのまま維持され、対応するインターフェイスが **shutdown** コマンドを使用して設定された場合でも、直接接続されたデバイスはアップであると認識されます。

例

次に、メイン インターフェイスをイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

次に、サブインターフェイスをイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

次に、サブインターフェイスをシャットダウンする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に対するすべての変換をリセットして、その結果として接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

sip address

DHCPv6 サーバを設定するときに、Session Initiation Protocol（SIP）サーバ IP アドレスをステートレス アドレス自動設定（SLAAC）クライアントに提供するには、ipv6 dhcp プール コンフィギュレーション モードで **sip address** コマンドを使用します。SIP サーバを削除するには、このコマンドの **no** 形式を使用します。

sip address *sip_ipv6_address*

no sip address *sip_ipv6_address*

構文の説明

sip_ipv6_address	SIP サーバの IPv6 アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、SIP サーバを含め、**ipv6 dhcp プール**内の情報を提供するように ASA を設定できます。ASA は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。DHCPv6 ステートレス サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    dns-server 2001:DB8:1::1
    sip domain-name eng.example.com
    sip server 2001:DB8:2::8
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    dns-server 2001:DB8:1::1
    sip domain-name it.example.com
    sip server 2001:DB8:2::8
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。

コマンド	説明
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

sip domain-name

DHCPv6 サーバを設定するときに、Session Initiation Protocol（SIP）ドメイン名をステートレス アドレス自動設定（SLAAC）クライアントに提供するには、ipv6 dhcp プール コンフィギュレーション モードで **sip domain-name** コマンドを使用します。SIP ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

sip domain-name *sip_domain_name*

no sip domain-name *sip_domain_name*

構文の説明

sip_domain_name	SIP ドメイン名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、SIP ドメイン名を含め、**ipv6 dhcp プール**内の情報を提供するように ASA を設定できます。ASA は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。DHCPv6 ステートレス サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    dns-server 2001:DB8:1::1
    sip domain-name eng.example.com
    sip server 2001:DB8:2::8
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    dns-server 2001:DB8:1::1
    sip domain-name it.example.com
    sip server 2001:DB8:2::8
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。

コマンド	説明
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

site-id

サイト間クラスタリングの場合は、クラスタ グループ コンフィギュレーション モードで **site-id** コマンドを使用します。サイト ID を削除するには、このコマンドの **no** 形式を使用します。

site-id *number*

no site-id *number*

構文の説明

number	1 ～ 8 の範囲でサイト ID を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。
9.5(2)	LISP フロー モビリティとともに使用するために、トランスペアレント モードでこのコマンドを入力できるようになりました。
9.7(1)	FXOS では、FXOS 論理デバイス設定でサイト ID を設定する必要があります。ASA では変更できません。

使用上のガイドライン

各クラスタ シャーシを、個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスで動作します。ASA クラスタから送信されたパケットはサイト固有の MAC アドレスを使用しますが、クラスタによって受信されるパケットはグローバル MAC アドレスを使用します。この機能により、スイッチが 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスを学習してしまうのを防いでいます。MAC フラッピングが発生しないよう、サイト MAC アドレスのみを学習します。サイト固有の MAC アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされています。

また、サイト ID は LISP インスペクションを使用するフロー モビリティを有効にするためにも使用されます。

マスター ユニットに MAC アドレスを設定するには、**mac-address site-id** コマンドを使用し、その後、**site-id** コマンドを使用して、各ユニット(マスターとスレーブ)をクラスタ ブートストラップ設定の一部としてサイトに割り当てます。

例

次に、port-channel 2 のサイト固有の MAC アドレスを設定して、マスター ユニットをサイト 1 に割り当てる例を示します。

```
ciscoasa(config)# interface port-channel 2
ciscoasa(config-if)# port-channel span-cluster
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4

ciscoasa(config)# cluster group pod1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# enable noconfirm
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable(クラスタ グループ)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mac-address site-id	各サイトのサイト固有の MAC アドレスを設定します。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。

site-periodic-garp interval

クラスタリングのための gratuitous ARP (GARP) 間隔をカスタマイズするには、クラスタ グループ コンフィギュレーション モードで **site-periodic-garp interval** コマンドを使用します。GARP をディセーブルにするには、このコマンドの **no** 形式を使用します。

site-periodic-garp interval *seconds*

no site-periodic-garp interval

構文の説明

seconds	GARP 生成の間隔を 1 ～ 1000000 秒間の秒単位で設定します。デフォルトは 290 秒です。

コマンド デフォルト

デフォルトの間隔は 290 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.12(1)	コマンドが追加されました。

使用上のガイドライン

ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保ちます。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。

クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチング インフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。

各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。

例

次に、GARP 間隔を 500 秒に設定する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# site-periodic-garp interval 500
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループ モードを開始します。

site-redundancy

サイトの障害からクラスタのフローを保護するには、クラスタ グループ コンフィギュレーション モードで **site-redundancy** コマンドを使用します。サイトの冗長性を無効にするには、このコマンドの **no** 形式を使用します。

site-redundancy

no site-redundancy

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

サイトの冗長性は、デフォルトで無効です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.9(1)	コマンドが追加されました。

使用上のガイドライン

サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。接続バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。

ディレクタ ローカリゼーションとサイトの冗長性は別々の機能です。そのうちの 1 つまたは両方を設定することができます。

例

次に、間隔を 300 ミリ秒に設定する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# site-redundancy
```

関連コマンド

コマンド	説明
director-localization	ディレクタ ローカリゼーションを有効にします。これによりパフォーマンスが向上し、データ センターのサイト間クラスタリングでラウンドトリップ時間の遅延が減少します。

sla monitor

SLA 動作を作成するには、グローバル コンフィギュレーション モードで **sla monitor** コマンドを使用します。SLA 動作を削除するには、このコマンドの **no** 形式を使用します。

sla monitor *sla_id*

no sla monitor *sla_id*

構文の説明

sla_id	設定する SLA の ID を指定します。SLA が存在しない場合は、作成されます。有効な値は 1 ～ 2147483647 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

sla monitor コマンドによって、SLA 動作が作成され、SLA モニタ コンフィギュレーション モードが開始されます。このコマンドを入力すると、コマンド プロンプトは `ciscoasa(config-sla-monitor)#` に変わり、SLA モニタ コンフィギュレーション モードになったことが示されます。SLA 動作がすでに存在し、それに対してタイプがすでに定義されている場合、プロンプトは `ciscoasa(config-sla-monitor-echo)#` と表示されます。最大 2000 個の SLA 動作を作成できます。任意の時点でデバッグできるのは 32 個の SLA 動作のみです。

no sla monitor コマンドによって、指定した SLA 動作およびその動作を設定するために使用されたコマンドが削除されます。

SLA 動作を設定した後、**sla monitor schedule** コマンドで動作をスケジューリングする必要があります。スケジューリング後は、SLA 動作のコンフィギュレーションを変更できません。スケジューリングした SLA 動作のコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択した SLA 動作を完全に削除する必要があります。SLA 動作を削除すると、関連づけられた **sla monitor schedule** コマンドも削除されます。その後、SLA 動作のコンフィギュレーションを再入力できます。

動作の現在のコンフィギュレーション設定を表示するには、**show sla monitor configuration** コマンドを使用します。SLA 動作の動作統計情報を表示するには、**show sla monitor operation-state** コマンドを使用します。コンフィギュレーション内の SLA コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA 動作を繰り返す頻度を指定します。
show sla monitor configuration	SLA コンフィギュレーション設定を表示します。
sla monitor schedule	SLA 動作をスケジューリングします。
timeout	SLA 動作が応答を待機する時間を設定します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

sla monitor schedule

SLA 動作をスケジューリングするには、グローバル コンフィギュレーション モードで **sla monitor schedule** コマンドを使用します。SLA 動作のスケジュールを削除し、動作を保留状態にするには、このコマンドの **no** 形式を使用します。

sla monitor schedule *sla-id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no sla monitor schedule *sla-id*

構文の説明

after *hh*:*mm*:*ss*	コマンドの入力後、何時間、何分、何秒で動作が開始されるかを示します。
ageout *seconds*	（任意）情報をアクティブに収集していない場合、動作をメモリに常駐させておく時間を秒数で指定します。エージング アウト後、SLA 動作は実行コンフィギュレーションから削除されます。
day	動作を開始する日。有効な値は、1 ～ 31 です。日を指定しない場合、現在の日が使用されます。日を指定する場合は、月も指定する必要があります。
hh:*mm*[:*ss*]	絶対開始時刻を 24 時間表記で指定します。秒は任意です。*month* および *day* を指定しない場合は、指定した時刻が次に来たときとなります。
life forever	（任意）無期限に実行されるように動作をスケジューリングします。
life *seconds*	（任意）動作によって情報がアクティブに収集される秒数を設定します。
month	（オプション）動作を開始する月の名前。月を指定しない場合は、現在の月が使用されます。月を指定する場合は、日も指定する必要があります。 月の英語名を完全に入力するか、または、最初の 3 文字のみを入力します。
now	コマンドを入力するとすぐに動作が開始されることを示します。
pending	情報が収集されないことを示します。これは、デフォルトの状態です。
recurring	（任意）動作が毎日、指定した時刻に自動的に開始され、指定した時間継続されることを示します。
sla-id	スケジューリングする SLA 動作の ID。
start-time	SLA 動作が開始される時刻を設定します。

デフォルト

デフォルトの設定は次のとおりです。

- SLA 動作は、スケジューリングされた時間になるまで **pending** 状態です。つまり、動作はイネーブルですが、データはアクティブに収集されていません。
- デフォルトの **ageout** 時間は、0 秒（エージング アウトしない）です。
- デフォルトの **life** は、3600 秒（1 時間）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

SLA 動作がアクティブ状態の場合、ただちに情報の収集が開始されます。次のタイム ラインは、動作のエージング アウト プロセスを示しています。

```
W----------------------X----------------------Y----------------------Z
```

- W は、SLA 動作が **sla monitor** コマンドで設定された時刻です。
- X は、SLA 動作の開始時刻です。これは、動作が「アクティブ」になったときです。
- Y は、**sla monitor schedule** コマンドで設定された有効期間の終了です（**life** の秒数は 0 までカウント減少されました）。
- Z は、動作のエージング アウトです。

エージ アウト プロセスは、使用されている場合は、W でカウント ダウンを開始し、X と Y の間は中断され、設定されたサイズにリセットされると、再び Y でカウント ダウンを開始します。SLA 動作がエージ アウトすると、SLA 動作の設定は実行コンフィギュレーションから削除されます。動作は、実行される前にエージング アウトする可能性があります（つまり、Z が X の前に発生する可能性があります）。このような状況が発生しないようにするには、動作のコンフィギュレーション時刻と開始時刻（X と W）の差を、エージング アウトの秒数よりも小さくする必要があります。

recurring キーワードは、単一の SLA 動作のスケジューリングに対してのみサポートされています。1 つの **sla monitor schedule** コマンドを使用して複数の SLA 動作をスケジューリングすることはできません。定期的な SLA 動作の **life** 値は、1 日未満にする必要があります。定期的な動作の **ageout** 値を「なし」（値 0 で指定）にするか、**life** 値と **ageout** 値の合計を 1 日よりも大きくする必要があります。recurring オプションを指定しないと、動作は既存の通常のスケジューリング モードで開始されます。

スケジューリング後は、SLA 動作のコンフィギュレーションを変更できません。スケジューリングした SLA 動作のコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択した SLA 動作を完全に削除する必要があります。SLA 動作を削除すると、関連づけられた **sla monitor schedule** コマンドも削除されます。その後、SLA 動作のコンフィギュレーションを再入力できます。

例

次に、4 月 5 日午後 3 時にデータの収集をアクティブに開始するようにスケジューリングされた SLA 動作 25 の例を示します。この動作は、非アクティブになって 12 時間後にエージング アウトします。この SLA 動作がエージング アウトすると、SLA 動作のすべてのコンフィギュレーション情報は実行コンフィギュレーションから削除されます。

```
ciscoasa(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

次に、5 分間の遅延の後にデータの収集を開始するようにスケジューリングされた SLA 動作 1 の例を示します。デフォルトの有効期間である 1 時間が適用されます。

```
ciscoasa(config)# sla monitor schedule 1 start after 00:05:00
```

次に、ただちにデータの収集を開始するようにスケジューリングされた SLA 動作 3 の例を示します。この例は、無期限に実行されるようにスケジューリングされています。

```
ciscoasa(config)# sla monitor schedule 3 life forever start-time now
```

次に、毎日午前 1 時 30 分にデータの収集を自動的に開始するようにスケジューリングされた SLA 動作 15 の例を示します。

```
ciscoasa(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

関連コマンド

コマンド	説明
show sla monitor configuration	SLA コンフィギュレーション設定を表示します。
sla monitor	SLA モニタリング動作を定義します。

smart-tunnel auto-signon enable

クライアントレス(ブラウザベース)SSL VPN セッションでスマート トンネル自動サインオンをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel auto-signon enable** コマンドを使用します。

グループ ポリシーまたはユーザ名から **smart-tunnel auto-signon enable** コマンドを削除し、デフォルトのグループ ポリシーから継承するには、このコマンドの **no** 形式を使用します。

no smart-tunnel auto-signon enable *list* [**domain** *domain*] [port *port*] [realm *realm string*]

構文の説明

domain *domain*	(任意)。認証中にユーザ名に追加されるドメインの名前。ドメインを入力する場合、**use-domain** キーワードをリスト エントリに入力します。
list	ASA の webvpn コンフィギュレーションにすでに存在するスマート トンネル自動サインオン リストの名前。 SSL VPN コンフィギュレーション内のスマート トンネル自動サインオン リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。
port	自動サインオンを実行するポートを指定します。
レルム	認証のレルムを設定します。

デフォルト

このコマンドにデフォルトはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
8.4(1)	オプションの *realm* 引数と *port* 引数が追加されました。

使用上のガイドライン

スマート トンネル自動サインオン機能は、Microsoft WININET ライブラリを使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。

smart-tunnel auto-signon *list* コマンドを使用して、最初にサーバのリストを作成する必要があります。グループ ポリシーまたはユーザ名に割り当てることができるリストは 1 つだけです。

レルムの文字列は Web サイトの保護領域に関連付けられ、認証時に認証プロンプトまたは HTTP ヘッダーのいずれかでブラウザに再度渡されます。対応するレルムがわからない場合、管理者はログインを一度実行し、プロンプト ダイアログから文字列を取得する必要があります。

管理者は、対応するホストに任意でポート番号を指定できるようになりました。Firefox では、ポート番号が指定されていない場合、自動サインオンはデフォルトのポート番号 80 および 443 でそれぞれアクセスされた HTTP および HTTPS に対して実行されます。

例

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをイネーブルにします。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR
ciscoasa(config-group-webvpn)
```

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをイネーブルにし、認証中に CISCO という名前のドメインをユーザ名に追加します。

```
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル自動サインオン リスト コマンドを継承します。

```
ciscoasa(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

関連コマンド

コマンド	説明
smart-tunnel auto-signon *list*	スマート トンネル接続でクレデンシャルの送信を自動化する対象のサーバのリストを作成します。
show running-config webvpn smart-tunnel	ASA のスマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel *list*	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel auto-signon list

スマート トンネル接続でクレデンシャルの送信を自動化する対象のサーバのリストを作成するには、webvpn コンフィギュレーション モードで **smart-tunnel auto-signon list** コマンドを使用します。リストに追加する各サーバに対してこのコマンドを使用します。

リストからエントリを削除するには、このコマンドの **no** 形式を使用します。リストと、ASA コンフィギュレーションに表示されている IP アドレスまたはホスト名を指定します。

no smart-tunnel auto-signon *list* [**use-domain**] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

スマート トンネル自動サインオン リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。

サーバのリスト全体を ASA コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用して、リストのみを指定します。

no smart-tunnel auto-signon *list*

構文の説明

ホスト	ホスト名またはワイルドカード マスクによって識別されるサーバ。
hostname-mask	自動認証する対象のホスト名またはワイルドカード マスク。
ip	IP アドレスおよびネット マスクによって識別されるサーバ。
ip-address [*netmask*]	自動認証する対象のホストのサブネットワーク。
list	リモート サーバのリストの名前。スペースを含む場合、名前の前後に引用符を使用します。文字列は最大 64 文字まで使用できます。コンフィギュレーション内にリストが存在しない場合は、ASA によって作成されます。存在する場合、リストにエントリを追加します。
use-domain	(任意)認証で必要な場合、Windows ドメインをユーザ名に追加します。このキーワードを入力する場合は、スマート トンネル リストを 1 つ以上のグループ ポリシーまたはユーザ名に割り当てるときにドメイン名を指定してください。

デフォルト

このコマンドにデフォルトはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

スマート トンネル自動サインオン機能は、Microsoft WININET ライブラリを使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。

スマート トンネル自動サインオン リストの入力に続き、グループ ポリシー webvpn モードまたはユーザ名 webvpn モードで **smart-tunnel auto-signon enable** *list* コマンドを使用してリストを割り当てます。

例

次のコマンドでは、サブネット内のすべてのホストを追加し、認証で必要な場合に Windows ドメインをユーザ名に追加します。

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

次のコマンドは、リストからエントリを削除します。

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

前述のコマンドでは、削除されるエントリがリストの唯一のエントリである場合、HR という名前のリストも削除されます。唯一のエントリではない場合は、次のコマンドによってリスト全体が ASA コンフィギュレーションから削除されます。

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR
```

次のコマンドでは、ドメイン内のすべてのホストを intranet という名前のスマート トンネル自動サインオン リストに追加します。

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

次のコマンドは、リストからエントリを削除します。

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon intranet host *.exampledomain.com
```

関連コマンド

コマンド	説明
smart-tunnel auto-signon enable	コマンド モードで指定されたグループ ポリシーまたはユーザ名に対して、スマート トンネル自動サインオンをイネーブルにします。
smart-tunnel auto-signon enable *list*	グループ ポリシーまたはユーザ名にスマート トンネル自動サインオン リストを割り当てます。
show running-config webvpn smart-tunnel	スマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。

smart-tunnel auto-start

クライアントレス（ブラウザベース）SSL VPN セッションでユーザがログインしたときにスマート トンネル アクセスを自動的に開始するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel auto-start** コマンドを使用します。

smart-tunnel auto-start *list*

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除し、デフォルト グループ ポリシーの [**no**] **smart-tunnel** コマンドを継承するには、コマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

list	*list* は、ASA webvpn コンフィギュレーションにすでに存在するスマート トンネル リストの名前です。 SSL VPN コンフィギュレーション内にすでに存在するスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、**smart-tunnel list** コマンドを使用して、最初にアプリケーションのリストを作成する必要があります。

ユーザのログイン時にスマート トンネル アクセスを開始するこのオプションは Windows だけに適用されます。

例

次のコマンドでは、apps1 という名前のアプリケーションのリストについて、スマート トンネル アクセスを開始します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-start apps1
ciscoasa(config-group-webvpn)
```

次のコマンドでは、apps1 という名前のリストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル コマンドを継承します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN コンフィギュレーションを、すべてのスマート トンネル リスト エントリを含めて表示します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel disable

クライアントレス(ブラウザベース)SSL VPN セッションでスマート トンネル アクセスを禁止するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel disable** コマンドを使用します。

smart-tunnel disable

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除して、デフォルトのグループ ポリシーから **[no] smart-tunnel** コマンドを継承するには、このコマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

デフォルトではスマート トンネルはイネーブルではないため、**smart-tunnel disable** コマンドは(デフォルトの)グループ ポリシーまたはユーザ名コンフィギュレーションに、対象のポリシーまたはユーザ名に適用しない **smart-tunnel auto-start** または **smart-tunnel enable** コマンドが含まれている場合にのみ必要です。

例

次のコマンドでは、スマート トンネル アクセスを禁止します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel disable
ciscoasa(config-group-webvpn)
```

関連コマンド

コマンド	説明
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel enable

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル アクセスをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel enable** コマンドを使用します。

smart-tunnel enable *list*

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除し、デフォルト グループ ポリシーの **[no] smart-tunnel** コマンドを継承するには、コマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

list	*list* は、ASA webvpn コンフィギュレーションにすでに存在するスマート トンネル リストの名前です。 SSL VPN コンフィギュレーション内のスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

smart-tunnel enable コマンドによって、スマート トンネル アクセスに適格なアプリケーションのリストがグループ ポリシーまたはユーザ名に割り当てられます。ユーザは、クライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。または、**smart-tunnel auto-start** コマンドを使用して、ユーザがログインしたときに自動的にスマート トンネル アクセスを開始できます。

いずれのコマンドでも、**smart-tunnel list** コマンドを使用して、最初にアプリケーションのリストを作成する必要があります。

例

次のコマンドでは、apps1 という名前のスマート トンネル リストをイネーブルにします。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel enable apps1
ciscoasa(config-group-webvpn)
```

次のコマンドでは、apps1 という名前のリストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル リストを継承します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN コンフィギュレーションを、すべてのスマート トンネル リスト エントリを含めて表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel list

プライベート サイトに接続する場合にクライアントレス（ブラウザベース）SSL VPN セッションを使用できるアプリケーションのリストに入力するには、webvpn コンフィギュレーション モードで **smart-tunnel list** コマンドを使用します。アプリケーションをリストから削除するには、このコマンドの **no** 形式を使用して、エントリを指定します。アプリケーションのリスト全体を ASA コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用して、リストだけを指定します。

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]

no smart-tunnel list *list*

構文の説明

application	スマート トンネル アクセスが付与されるアプリケーションの名前。文字列は最大 64 文字まで使用できます。
hash	（任意。Windows にのみ該当）この値を取得するには、アプリケーションのチェックサム（つまり、実行ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュを計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft ファイル チェックサム整合性検証（FCIV）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。FCIV のインストール後、スペースを含まないパス（c:/fciv.exe など）に、ハッシュするアプリケーションの一時コピーを置き、コマンドラインで **fciv.exe -sha1** *application* と入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。 SHA-1 ハッシュは、常に 16 進数 40 文字です。
list	アプリケーションまたはプログラムのリストの名前。スペースを含む場合、名前の前後に引用符を使用します。コンフィギュレーション内にリストが存在しない場合は、CLI によって作成されます。存在する場合、リストにエントリを追加します。
path	Mac OS の場合は、アプリケーションのフル パス。Windows の場合は、アプリケーションのファイル名。または、ファイル名を含むアプリケーションのフル パスまたは部分パス。ストリングには最大 128 文字を使用できます。
platform *OS*	（OS が Microsoft Windows の場合は任意）**windows または mac** を入力して、アプリケーションのホストを指定します。

デフォルト

Windows がデフォルトのプラットフォームです。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)	**platform** *OS* が追加されました。

使用上のガイドライン　複数のスマート トンネル リストを ASA で設定できますが、複数のスマート トンネル リストを特定のグループ ポリシーまたはユーザ名に割り当てることはできません。スマート トンネル リストに入力するには、アプリケーションごとに **smart-tunnel list** コマンドを 1 回入力します。同じ *list* ストリングを入力しますが、OS で一意の *application* および *path* を指定します。リストでサポートする各 *OS* について、コマンドを 1 回入力します。

OS がエントリで指定されたものと一致しない場合、セッションでリスト エントリは無視されます。アプリケーションのパスが存在しない場合も、エントリは無視されます。

SSL VPN コンフィギュレーション内のスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。

path はコンピュータ上のものと一致する必要がありますが、完全である必要はありません。たとえば、実行ファイルとその拡張子だけで *path* を構成できます。

スマート トンネルには次の要件があります。

- スマート トンネル接続を開始するリモート ホストでは、32 ビット バージョンの Microsoft Windows Vista、Windows XP、または Windows 2000、あるいは Mac OS 10.4 または 10.5 が実行されている必要があります。
- スマート トンネルまたはポート フォワーディングを使用する Microsoft Windows Vista のユーザは、ASA の URL を [Trusted Site] ゾーンに追加する必要があります。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動して、[Tools] > [Internet Options] > [Security] タブを選択する必要があります。Vista ユーザは、[Protected Mode] をディセーブルにしてスマート トンネル アクセスを容易にすることもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法は推奨しません。
- ブラウザで Java、Microsoft ActiveX、またはその両方をイネーブルにする必要があります。
- Mac OS のスマート トンネル サポートには、Safari 3.1.1 以降が必要です。

Microsoft Windows では、Winsock 2、TCP ベースのアプリケーションのみがスマート トンネル アクセスに適格です。

Mac OS では、SSL ライブラリにダイナミックにリンクされた、TCP を使用するアプリケーションをスマート トンネルで使用できます。次のタイプのアプリケーションは、スマート トンネルで使用できません。

- dlopen または dlsym を使用して libsocket コールを特定するアプリケーション
- libsocket コールを特定するためにスタティックにリンクされたアプリケーション
- 2 レベルのネーム スペースを使用する Mac OS アプリケーション。
- Mac OS のコンソールベースのアプリケーション（Telnet、SSH、cURL など）。
- Mac OS の PowerPC タイプのアプリケーション。Mac OS アプリケーションのタイプを判別するには、そのアイコンを右クリックして [Get Info] を選択します。

Mac OS では、ポータル ページから起動されたアプリケーションだけがスマート トンネル セッションを確立できます。この要件には、Firefox に対するスマート トンネルのサポートも含まれます。スマート トンネルを最初に使用する際に、Firefox を使用して Firefox の別のインスタンスを起動するには、csco_st という名前のユーザ プロファイルが必要です。このユーザ プロファイルが存在しない場合、セッションでは、作成するようにユーザに要求します。

次の制限事項がスマート トンネルに適用されます。

- リモート コンピュータが ASA にアクセスするためにプロキシ サーバを必要とする場合、接続の終端側の URL が、プロキシ サービスから除外される URL のリストに存在する必要があります。この設定では、スマート トンネルは基本認証だけをサポートします。
- スマート トンネル自動サインオン機能では、Microsoft Windows OS 上の Microsoft WININET ライブラリを使用して HTTP または HTTPS 通信を行うアプリケーションのみがサポートされます。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。
- グループ ポリシーまたはローカル ユーザ ポリシーでは、スマート トンネル アクセスに適格なアプリケーションのリスト 1 つと、スマート トンネル自動サインオン サーバのリスト 1 つだけがサポートされます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されません。ユーザはフェールオーバー後に再接続する必要があります。

(注) スマート トンネル アクセスで突然問題が発生した場合、アプリケーションのアップグレードにより、*path* 値が最新でないことを示している場合があります。たとえば、アプリケーションおよび次のアップグレードを作成する会社が買収されると、アプリケーションのデフォルトのパスは通常は変更されます。

ハッシュを入力すると、*path* で指定したストリングと一致する不適格なファイルがクライアントレス SSL VPN によって認定されないことが、ある程度保証されます。チェックサムはアプリケーションの各バージョンまたはパッチによって異なるため、入力する *hash* が一致するのは、リモート ホスト上の 1 つのバージョンまたはパッチのみです。アプリケーションの複数のバージョンに対して *hash* を指定するには、各バージョンに対して **smart-tunnel list** コマンドを 1 回入力します。このとき、各コマンドでは、同じ *list* ストリングを入力しますが、一意の *application* ストリングと一意の *hash* 値を指定します。

(注) *hash* 値を入力し、スマート トンネル アクセスでアプリケーションの今後のバージョンまたはパッチをサポートする場合は、今後もスマート トンネル リストを維持する必要があります。スマート トンネル アクセスで突然問題が発生した場合、アプリケーションのアップグレードにより、*hash* 値を含むアプリケーション リストが最新でないことを示している場合があります。この問題は *hash* を入力しないことによって回避できます。

スマート トンネル リストのコンフィギュレーションに続き、**smart-tunnel auto-start** または **smart-tunnel enable** コマンドを使用して、グループ ポリシーまたはユーザ名にリストを割り当てます。

例

次のコマンドでは、apps1 という名前のスマート トンネル リストに Microsoft Windows アプリケーションの接続を追加します。

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

次のコマンドでは、Windows アプリケーション msimn.exe を追加し、リモート ホスト上のアプリケーションのハッシュが、スマート トンネル アクセスを許可するために入力された最後のストリングと一致することを要求します。

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

次のコマンドでは、Mac OS ブラウザ Safari にスマート トンネル サポートを提供します。

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform mac
```

関連コマンド

コマンド	説明
show running-config webvpn smart-tunnel	ASA のスマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。

smart-tunnel network

スマート トンネル ポリシーの設定に使用するホストのリストを作成するには、webvpn コンフィギュレーション モードで **smart-tunnel network** コマンドを使用します。スマート トンネル ポリシー用ホストのリストを不許可にするには、このコマンドの **no** 形式を使用します。

smart-tunnel network

no smart-tunnel network

構文の説明

host *host mask*	ホスト名（*.cisco.com など）。
ip *ip address*	ネットワークの IP アドレス。
netmask	ネットワークのネットマスク。
network name	トンネル ポリシーに適用するネットワーク名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

スマート トンネルがオンになっている場合、ネットワーク（ホストのセット）を設定する **smart-tunnel network** コマンド、および指定されたスマート トンネル ネットワークを使用してポリシーをユーザに強制適用する **smart-tunnel tunnel-policy** コマンドによって、トンネル外のトラフィックを許可できます。

例

次に、**smart-tunnel network** コマンドの使用例を示します。

```
ciscoasa(config-webvpn)# smart-tunnel network testnet ip 192.168.0.0 255.255.255
```

関連コマンド

コマンド	説明
smart-tunnel tunnel-policy	指定されたスマート トンネル ネットワークを使用してポリシーをユーザに強制適用します。

smart-tunnel tunnel-policy

スマート トンネル トンネル ポリシーを特定のグループ ポリシーまたはユーザ ポリシーに適用するには、コンフィギュレーション webvpn モードで **smart-tunnel tunnel-policy** コマンドを使用します。特定のグループからスマート トンネル トンネル ポリシーの適用をはずすには、このコマンドの [no] 形式を使用します。

smart-tunnel tunnel-policy

no smart-tunnel tunnel-policy

構文の説明

excludespecified	ネットワーク名で指定されたネットワークの外のネットワークだけをトンネリングします。
network name	トンネリングするネットワークをリストします。
tunnelall	すべてをトンネリング（暗号化）します。
tunnelspecified	ネットワーク名で指定されたネットワークだけをトンネリングします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3.1	このコマンドが追加されました。

使用上のガイドライン

スマート トンネルがオンになっている場合、ネットワーク（ホストのセット）を設定する **smart-tunnel network** コマンド、および指定されたスマート トンネル ネットワークを使用してポリシーをユーザに強制適用する **smart-tunnel tunnel-policy** コマンドによって、トンネル外のトラフィックを許可できます。

例

次に、**smart-tunnel tunnel-policy** コマンドの使用方法の例を示します。

```
ciscoasa(config-username-webvpn)# smart-tunnel tunnel-policy tunnelspecified testnet
```

関連コマンド

コマンド	説明
smart-tunnel network	スマート トンネル ポリシー設定のためホストのリストを作成します。

smtp from-address

ローカル CA サーバが生成するすべての電子メール（ワンタイム パスワードの配布など）の送信者フィールドで使用する電子メール アドレスを指定するには、CA サーバ コンフィギュレーション モードで **smtp from-address** コマンドを使用します。電子メール アドレスをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

smtp from-address *e-mail_address*

no smtp from-address

構文の説明

e-mail_address	CA サーバが生成するすべての電子メールの送信者フィールドに表示する電子メール アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、ローカル CA サーバからの、すべての電子メールの送信者フィールドに ca-admin@asa1-ca.example.com が含まれるように指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address ca-admin@asa1-ca.example.com
ciscoasa(config-ca-server)#
```

次に、ローカル CA サーバからの、すべての電子メールの送信者フィールドをデフォルトのアドレス admin@asa1-ca.example.com にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address admin@asa1-ca.example.com
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示するテキストをカスタマイズします。

smtp subject

ローカル認証局(CA)サーバが生成するすべての電子メール(ワンタイム パスワードの配布など)の件名フィールドに表示するテキストをカスタマイズするには、CA サーバ コンフィギュレーション モードで **smtp subject** コマンドを使用します。テキストをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

smtp subject *subject-line*

no smtp subject

構文の説明

subject-line	CA サーバから送信するすべての電子メールの件名フィールドに表示するテキストを指定します。最大文字数は 127 です。

デフォルト

デフォルトでは、件名フィールドのテキストは「Certificate Enrollment Invitation」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、CA サーバからの、すべての電子メールの件名フィールドにテキスト *Action: Enroll for a certificate* を表示するように指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp subject Action: Enroll for a certificate
ciscoasa(config-ca-server)#
```

次に、CA サーバからの、すべての電子メールの件名フィールドのテキストをデフォルトのテキスト「Certificate Enrollment Invitation」にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no smtp subject
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
smtp from-address	ローカル CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。

smtps（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

SMTPS コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **smtps** コマンドを使用します。SMTPS コマンド モードで入力されたコマンドを削除するには、このコマンドの **no** 形式を使用します。SMTPS は、SSL 接続での電子メールの送信を可能にする TCP/IP プロトコルです。

smtps

no smtps

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

例

次に、SMTPS コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# smtps
ciscoasa(config-smtps)#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
show running-config smtps	SMTPS の実行コンフィギュレーションを表示します。

smtp-server

SMTP サーバを設定するには、グローバル コンフィギュレーション モードで **smtp-server** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

smtp-server [*primary-interface*] *primary-smpt-server-ip-address*) [[*backup-interface*] *backup-smpt-server-ip-address*]

no smtp-server

構文の説明

primary-smpt-server-ip-address	プライマリ SMTP サーバを指定します。IP アドレスまたはホスト名（**name** コマンドを使用して設定）を使用します。
backup-smpt-server-ip-address	（オプション）プライマリ SMTP サーバが利用できない場合にイベント メッセージをリレーするバックアップ SMTP サーバを指定します。IP アドレスまたはホスト名（**name** コマンドを使用して設定）を使用します。
primary_interface	（オプション）プライマリ smtp サーバに到達するために使用できるプライマリ インターフェイス名を指定します。
backup_interface	（オプション）バックアップ smtp サーバに到達するために使用できるバックアップ インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。
9.13(1)	ロギングのための適切な smtp サーバに接続するために、プライマリおよびバックアップのインターフェイス名を任意で指定できます。

使用上のガイドライン

ASA には、内部 SMTP クライアントが含まれており、特定のイベントが発生したことを外部エンティティに通知するためにイベント システムで使用できます。これらのイベント通知を受信し、指定された電子メール アドレスに転送するように SMTP サーバを設定できます。ASA に対して電子メール イベントをイネーブルにしている場合にのみ、SMTP ファシリティはアクティブです。また、このコマンドにより、ロギングに使用するルーティング テーブル（管理ルーティング テーブルまたはデータ ルーティング テーブル）をインターフェイス アソシエーションで識別できるようにします。インターフェイスが指定されていない場合、ASA は管理ルーティング テーブル ルックアップを参照し、適切なルート エントリが存在しない場合は、データ ルーティング テーブルを参照します。

例

次に、SMTP サーバを IP アドレス 10.1.1.24 を使用して設定し、バックアップ SMTP サーバを IP アドレス 10.1.1.34 を使用して設定する例を示します。

```
ciscoasa(config)# smtp-server 10.1.1.24 10.1.1.34
ciscoasa(config)# smtp-server 10.1.1.24
ciscoasa(config)# smtp-server management 10.1.1.24 outside 10.1.1.34
ciscoasa(config)# smtp-server management 10.1.1.24
```

snmp cpu threshold rising

高 CPU しきい値およびしきい値モニタリング期間のしきい値を設定するには、グローバル コンフィギュレーション モードで **snmp cpu threshold rising** コマンドを使用します。しきい値およびしきい値モニタリング期間を設定しない場合は、このコマンドの **no** 形式を使用します。

snmp cpu threshold rising *threshold_value monitoring_period*

no snmp cpu threshold rising *threshold_value monitoring_period*

構文の説明

monitoring_period	モニタリング期間を分単位で定義します。
threshold_value	しきい値レベルを CPU 使用率として定義します。

デフォルト

snmp cpu threshold rising コマンドが設定されていない場合、上限しきい値レベルのデフォルトは 70% の CPU 使用率を超えて設定されます。クリティカルしきい値レベルのデフォルトは 95% の CPU 使用率を超えて設定されます。デフォルトのモニタリング期間は 1 分に設定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。ASA サービス モジュール には適用されません。

使用上のガイドライン

CPU のクリティカルしきい値レベルは設定できません。この値は 95% に固定されています。有効なしきい値の範囲は 10 ～ 94% の CPU 使用率です。モニタリング期間の有効値は 1～60 分です。

例

次に、SNMP CPU しきい値レベルを 75% の CPU 使用率および 30 分のモニタリング期間に設定する例を示します。

```
ciscoasa(config)# snmp cpu threshold 75% 30
```

関連コマンド

コマンド	説明
snmp-server enable traps	SNMP-related トラップをイネーブルにします。
snmp link threshold	SNMP インターフェイスのしきい値を定義します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp link threshold

SNMP 物理インターフェイスのしきい値およびシステム メモリ使用率のしきい値を設定するには、グローバル コンフィギュレーション モードで **snmp link threshold** コマンドを使用します。SNMP 物理インターフェイスのしきい値およびシステム メモリ使用率のしきい値をクリアするには、このコマンドの **no** 形式を使用します。

snmp link threshold *threshold_value*

no snmp link threshold *threshold_value*

構文の説明

threshold_value	しきい値を CPU 使用率として定義します。

デフォルト

snmp link threshold コマンドを設定しない場合、デフォルトのしきい値は CPU 使用率およびシステム メモリ使用率の 70% です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

有効なしきい値の範囲は物理インターフェイスの 30 ～ 99% です。**snmp link threshold** コマンドは、管理コンテキストでのみ使用できます。

例

次に、SNMP インターフェイスのしきい値をすべての物理インターフェイスの 75% に設定する例を示します。

```
ciscoasa(config)# snmp link threshold 75%
```

関連コマンド

コマンド	説明
snmp-server enable traps	SNMP-related トラップをイネーブルにします。
snmp cpu threshold rising	SNMP CPU しきい値を定義します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-map

SNMP インスペクションのパラメータを定義するための特定のマップを指定するには、グローバル コンフィギュレーション モードで **snmp-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

snmp-map *map_name*

no snmp-map *map_name*

構文の説明

map_name	SNMP マップ名です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

snmp-map コマンドを使用して、SNMP インスペクションのパラメータを定義するために使用する特定のマップを指定します。このコマンドを入力すると、SNMP マップ コンフィギュレーション モードが開始され、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。SNMP マップの定義後、**inspect snmp** コマンドを使用してマップをイネーブルにします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、**inspect** コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

例

次に、SNMP トラフィックを指定し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する例を示します。

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port
ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
```

```
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp
ciscoasa(config-pmap-c)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

snmp-server community

SNMP コミュニティ ストリングを設定するには、グローバル コンフィギュレーション モードで **snmp-server community** コマンドを使用します。SNMP コミュニティ ストリングを削除するには、このコマンドの **no** 形式を使用します。

snmp-server community [*0* | *8*] *community-string*

no snmp-server community [*0* | *8*] *community-string*

構文の説明

0	(任意)暗号化されていない(クリア テキストの)コミュニティ ストリングが続くことを指定します。
8	暗号化されたコミュニティ ストリングが続くことを指定します。
community-string	SNMP コミュニティ ストリングを設定します。暗号化されたパスワード、または非暗号化(クリア テキスト)フォーマットのパスワードです。このコミュニティ ストリングは最大 32 文字です。

デフォルト

デフォルトのコミュニティ ストリングは「public」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	*text* 引数が *community-string* 引数に変更されました。
8.3(1)	暗号化パスワードのサポートが追加されました。

使用上のガイドライン

SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理されるネットワーク ノード間の共有秘密です。管理ステーションとデバイス間のバージョン 1 およびバージョン 2c の通信に対してのみ使用されます。ASA では、キーを使用して着信 SNMP 要求が有効かどうかを判別します。

たとえば、あるサイトにコミュニティ ストリングを指定し、さらに同じストリングを使用してルータ、ASA、管理ステーションを設定できます。ASA はこのストリングを使用し、無効なコミュニティ ストリングを持つ要求には応答しません。

暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。

暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

（注） ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリア テキストに戻してから結果を保存する必要があります。

例

次に、コミュニティ ストリングを「onceuponatime」に設定する例を示します。

```
ciscoasa(config)# snmp-server community onceuponatime
```

次の例では、暗号化されたコミュニティ ストリングを設定しています。

```
ciscoasa(config)# snmp-server community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

次の例では、非暗号化コミュニティ ストリングを設定しています。

```
ciscoasa(config)# snmp-server community 0 cisco
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP カウンタをクリアします。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server contact

SNMP サーバのコンタクト名を設定するには、グローバル コンフィギュレーション モードで **snmp-server contact** コマンドを使用します。SNMP のコンタクト名を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *text*

no snmp-server contact [*text*]

構文の説明

text	コンタクト担当者または ASA システム管理者の名前を指定します。名前は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、SNMP サーバのコンタクトを EmployeeA に設定する例を示します。

```
ciscoasa(config)# snmp-server contact EmployeeA
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable

ASA で SNMP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable** コマンドを使用します。SNMP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable

no snmp-server enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

SNMP サーバはイネーブルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

SNMP トラップまたはその他のコンフィギュレーションを設定および再設定しなくても、SNMP を簡単にイネーブルおよびディセーブルにすることができます。

例

次の例では、SNMP をイネーブルにし、SNMP ホストとトラップを設定してから、syslog メッセージとしてトラップを送信しています。

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable oid

ASA が SNMP ウォーク操作を通じて空きメモリと使用メモリの統計を照会できるようにするには、グローバル コンフィギュレーション モードで **snmp server enable oid** コマンドを使用します。メモリ統計情報のクエリをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable oid *mempool*

no snmp-server enable oid *mempool*

構文の説明

cisco-enhanced-mempool-mib	（オプション）SNMP ウォーク操作を実行するときにクエリする MIB オブジェクトを指定します。 *mempool* の排他 MIB オブジェクトには、次のものが含まれます。 • ciscoMemoryPoolUsed • ciscoMemoryPoolFree • cempMemPoolHCUsed • cempMemPoolHCFree

デフォルト

デフォルトでは、**snmp-server enable oid** は、これらの MIB オブジェクトの snmp ウォーク動作を可能にするためイネーブルになっています。

このコマンドの **no** 形式を使用して、これらの MIB オブジェクトをディセーブルにすることができます。**clear configure snmp-server** コマンドを使用すると、メモリのクエリのための SNMP MIB オブジェクトがデフォルトのイネーブル状態に戻ります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• なし	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

使用上のガイドライン

SNMP ウォークの操作を実行すると、ASA は MEMPOOL_DMA プールと MEMPOOL_GLOBAL_SHARED プールからメモリ情報を照会します。ASA がメモリ情報を照会すると、CPU は他のプロセスに開放される前に SNMP プロセスによって長時間にわたり保持されることがあります。これにより、SNMP 関連の CPU ホグ状態になり、パケットがドロップされることがあります。

この問題を軽減するには、**no snmp-server enable oid** コマンドを使用して、グローバル共有プールに関連する OID をポーリングしないようにしてください。ディセーブルにすると、*mempool* OID は 0 バイトを返します。ただし、このコマンドに関係なく、そのプールに対する GET 要求を使用して明示的にクエリすることができます。

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable traps

ASA の NMS へのトラップ送信をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。トラップをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **config** | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **ikev2** [*trap*] [...] | **remote-access** [*trap*] | **connection-limit-reached** | **cpu threshold rising** | **link-threshold** | **memory-threshold** | **nat** [*trap*]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **config** | **entity** [***trap***] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*] | **connection-limit-reached** | **cpu threshold rising** | **link-threshold** | **memory-threshold** | **nat** [*trap*]

構文の説明

all	すべてのトラップをイネーブルにします。
config	設定トラップをイネーブルにします。
connection-limit-reached	接続制限に達したトラップをイネーブルにします。
cpu threshold rising	CPU しきい値上限トラップをイネーブルにします。
entity [*trap*]	エンティティ トラップをイネーブルにします。**entity** トラップは次のとおりです。 • **accelerator-temperature** • **chassis-fan-failure** • **chassis-temperature** • **config-change** • **cpu-temperature** • **fan-failure** • **fru-insert** • **fru-remove** • **l1-bypass-status** • **power-supply** • **power-supply-failure** • **power-supply-presence** • **power-supply-temperature**
ipsec [*trap*]	IPsec トラップをイネーブルにします。**ipsec** トラップは次のとおりです。 • **start** • **stop**
ikev2 [*trap*]	IKEv2 IPsec トラップをイネーブルにします。**ikev2** トラップは次のとおりです。 • **start** • **stop**
link-threshold	リンクしきい値に達したトラップをイネーブルにします。

memory-threshold	メモリしきい値に達したトラップをイネーブルにします。
nat [*trap*]	NAT に関連するトラップをイネーブルにします。**nat** トラップは次のとおりです。 • **packet-discard**
remote-access [*trap*]	リモート アクセス トラップをイネーブルにします。**remote-access** トラップは次のとおりです。 • **session-threshold-exceeded**
snmp [*trap*]	SNMP トラップを有効にします。デフォルトでは、すべての SNMP トラップはイネーブルになっています。**snmp** トラップは次のとおりです。 • **authentication** • **linkup** • **linkdown** • **coldstart** • **warmstart**
syslog	syslog メッセージ トラップをイネーブルにします。

デフォルト

デフォルトのコンフィギュレーションでは、次の **snmp** トラップがイネーブルです（**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart**）。このコマンドを入力し、トラップ タイプを指定しない場合、デフォルトは **syslog** です（デフォルトの **snmp** トラップは **syslog** トラップとともに引き続きイネーブルのままです）。デフォルトでは他のトラップはすべてディセーブルです。

これらのトラップをディセーブルにするには、**snmp** キーワードを指定してこのコマンドの **no** 形式を使用します。**clear configure snmp-server** コマンドを使用すると、SNMP トラップのデフォルトのイネーブル状態に戻ります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	次のトラップが追加されました。**snmp warmstart**、**nat packet-discard**、**link-threshold**、**memory-threshold**、**entity power-supply**、**entity fan-failure**、**entity cpu-temperature**、**cpu threshold rising**、および **connection-limit-reached**。これらのトラップは ASASM には適用されません。

リリース	変更内容
8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために次のトラップが追加されました。**entity power-supply-failure**、**entity chassis-fan-failure**、**entity power-supply-presence**、**entity chassis-temperature**、および **entity power-supply-temperature**。
9.0(1)	IKEv2 および IPsec 用にマルチ コンテキスト モードのサポートが追加されました。
9.3(2)	次のトラップのサポートが追加されました。**config** および **entity accelerator-temperature**。

使用上のガイドライン

個別のトラップまたはトラップのセットをイネーブルにするには、機能タイプごとにこのコマンドを入力します。すべてのトラップをイネーブルにするには、**all** キーワードを入力します。

NMS にトラップを送信するには、**logging history** コマンドを入力し、**logging enable** コマンドを使用してロギングをイネーブルにします。

管理コンテキストのみで生成されるトラップは、次のとおりです。

- **connection-limit-reached**
- **entity**
- **memory-threshold**

システム コンテキストの物理的に接続されたインターフェイスに対してのみ管理コンテキストを介して生成されるトラップは、次のとおりです。

- **interface-threshold**

その他すべてのトラップは、管理およびユーザ コンテキストで使用できます。

accelerator-temperature しきい値トラップは、ASA 5506-X および ASA 5508-X にのみ適用されます。

chassis-fan-failure トラップは、ASA 5506-X には適用されません。

config トラップを指定すると、ciscoConfigManEvent 通知と ccmCLIRunningConfigChanged 通知がイネーブルになります。これらの通知は、コンフィギュレーション モードを終了した後に生成されます。

次のトラップは ASA 5506-X および ASA 5508-X には適用されません。**fan-failure**、**fru-insert**、**fru-remove**、**power-supply**、**power-supply-failure**、**power-supply-presence**、および **power-supply-temperature**。

マルチ コンテキスト モードのガイドライン

- マルチ コンテキスト モードでは、**fan-failure** トラップ、**power-supply-failure** トラップ、および **cpu-temperature** トラップは、ユーザ コンテキストではなく、管理コンテキストのみから生成されます。これらのトラップは、ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X にのみ適用され、ASA 5505 には適用されません。
- **snmp-server enable traps remote-access session-threshold-exceeded** コマンドは、マルチ コンテキスト モードではサポートされません。

CPU 使用率が、設定されたモニタリング期間の設定されたしきい値を超える場合、**cpu threshold rising** トラップが生成されます。

使用されたシステム メモリが 80% に達すると、**memory-threshold** トラップが生成されます。

(注) SNMP は電圧センサーをモニタしません。

例

次の例では、SNMP をイネーブルにし、SNMP ホストとトラップを設定してから、syslog メッセージとしてトラップを送信しています。

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server group

新しい SNMP グループを設定するには、グローバル コンフィギュレーション モードで **snmp-server group** コマンドを使用します。指定した SNMP グループを削除するには、このコマンドの **no** 形式を使用します。

snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

no snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

構文の説明

auth	暗号化を使用しないパケット認証を指定します。
group-name	グループの名前を指定します。
noauth	パケット認証を指定しません。
priv	暗号化されたパケット認証を指定します。
v3	グループが SNMP バージョン 3 セキュリティ モデルを使用することを指定します。このセキュリティ モデルは、サポートされているものの中で最もセキュアです。このバージョンでは、認証特性を明示的に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.3(1)	パスワード暗号化のサポートが追加されました。

使用上のガイドライン

バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定した後、SNMP ホストを設定する必要があります。バージョン 3 およびセキュリティ レベルも指定する必要があります。コミュニティ ストリングが内部的に設定されている場合、「public」という名前の 2 つのグループが自動的に作成されます。1 つはバージョン 1 セキュリティ モデル用、もう 1 つはバージョン 2c セキュリティ モデル用です。コミュニティ ストリングを削除すると、設定された両方のグループが自動的に削除されます。

(注) 特定のグループに属すように設定されるユーザは、グループと同じセキュリティ モデルを持つ必要があります。

ASA の起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

(注) ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリア テキストに戻してから結果を保存する必要があります。

例

次の例に、ASA が SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する方法について示します。これには、グループ、ユーザ、ホストの作成が含まれます。

```
ciscoasa(config)# snmp-server group vpn-group v3 priv
ciscoasa(config)# snmp-server user admin vpn-group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 admin
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP コンフィギュレーション カウンタをクリアします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server user	新しい SNMP ユーザを作成します。

snmp-server host

ASA で SNMP を使用可能な NMS を指定するには、グローバル コンフィギュレーション モードで **snmp-server host** コマンドを使用します。NMS をディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

no snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

構文の説明

0	(任意)暗号化されていない(クリア テキストの)コミュニティ ストリングが続くことを指定します。
8	暗号化されたコミュニティ ストリングが続くことを指定します。
community	NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。SNMP バージョン 1 または 2c でのみ有効です。
community-string	通知とともに、または NMS からの要求内で送信される、パスワードに似たコミュニティ ストリングを指定します。このコミュニティ ストリングは最大 32 文字です。暗号化フォーマットと非暗号化フォーマット(クリア テキスト)を使用できます。
hostname	SNMP 通知ホストを指定します。通常は NMS または SNMP マネージャです。
interface	NMS が ASA との通信に使用するインターフェイス名を指定します。
ip_address	SNMP トラップの送信先または SNMP 要求の送信元の NMS の IP アドレスを指定します。
poll	(任意)ホストはブラウズ(ポーリング)は可能だが、トラップは送信されないことを指定します。
port	NMS ホストの UDP ポート番号を設定します。
trap	(任意)トラップの送信のみが可能であり、このホストはブラウズ(ポーリング)できないことを指定します。
udp-port	(任意)SNMP トラップはデフォルト以外のポートで NMS ホストに送信される必要があることを指定します。
username	ホストに送信されるトラップ PDU に埋め込むユーザ名を指定します。SNMP バージョン 3 でのみ有効です。
version {**1** | **2c** | **3**}	(オプション)SNMP トラップ バージョンを指定します。ASA では、SNMP 要求(ポーリング)に基づくフィルタリングはサポートされません。

デフォルト

デフォルトの UDP ポートは 162 です。

デフォルトのバージョンは 1 です。

SNMP トラップはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	• SNMP バージョン 3 がサポートされています。 • *username* 引数が追加されました。 • *text* 引数が *community-string* 引数に変更されました。 • *interface_name* 引数が *interface* 引数に変更されました。
8.3(1)	暗号化パスワードのサポートが追加されました。
9.7(1)	直接接続された SNMP 管理ステーションがある場合、ASA および SNMP サーバの /31 サブネットを使用してポイントツーポイント接続を作成できます。
9.9(2)	IPv6 のサポートが追加されました。

使用上のガイドライン

現在使用中のポートで **snmp-server host** コマンドを設定すると、次のメッセージが表示されます。

警告 **UDP ポート *port* は、別の機能によって使用されています。異なるポートを使用するように snmp-server listen-port コマンドが設定されるまで、デバイスへの SNMP 要求は失敗します。**

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定し、SNMP ホストを設定する必要があります。ユーザ名はデバイス上で設定済みである必要があります。デバイスがフェールオーバー ペアのスタンバイ ユニットとして設定される場合、SNMP エンジン ID とユーザ コンフィギュレーションはアクティブ ユニットから複製されます。このアクションによって、SNMP バージョン 3 クエリーの観点から、トランスペアレントなスイッチオーバーが可能になります。スイッチオーバー イベントに対応するために NMS でのコンフィギュレーション変更は必要ありません。

暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。

暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

ASA の起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

(注) ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリア テキストに戻してから結果を保存する必要があります。

例

次に、ホストを内部インターフェイスに接続されている 192.0.2.5 に設定する例を示します。

```
ciscoasa(config)# snmp-server host inside 192.0.2.5
ciscoasa(config)# snmp-server host inside 192.0.2.5 version 3 username user1 password
cisco123 mschap md5aes128 udp-port 190
```

次に、ASA が SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する例を示します。これには、グループ、ユーザ、ホストの作成が含まれます。

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 username user1 password
cisco123 mschap priv admin
```

次に、暗号化されたコミュニティ ストリングを使用するようにホストを設定する例を示します。

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
username user1 password cisco123 mschap
```

次に、暗号化されていないコミュニティ ストリングを使用するようにホストを設定する例を示します。

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 0 cisco username user1 password
cisco123 mschap
```

次に、SNMP 通知バージョン 2c を使用して、ホストを IPv6 アドレス 12:ab:56:ce::11 に設定する例を示します。

```
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 community public version 2c
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP コンフィギュレーション カウンタをクリアします。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server group	新しい SNMP グループを設定します。
snmp-server user	新しい SNMP ユーザを設定します。

snmp-server host-group

ユーザ リストの 1 人のユーザまたはユーザ グループをネットワーク オブジェクトに関連付けるには、グローバル コンフィギュレーション モードで **snmp-server host-group** コマンドを使用します。アソシエーションを削除するには、このコマンドの **no** 形式を使用します。

snmp-server host-group *interface-network-object-name* [**trap** | **poll**]
[**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}]
[**udp-port** *port*]

no snmp-server host-group *interface-network-object-name* [**trap** | **poll**]
[**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}]
[**udp-port** *port*]

構文の説明

community	NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。SNMP バージョン 1 または 2c でのみ有効です。
community-string	通知とともに、または NMS からの要求内で送信される、パスワードに似たコミュニティ ストリングを指定します。このコミュニティ ストリングは最大 32 文字です。
interface-network-object-name	1 人のユーザまたはユーザ グループを関連付けるインターフェイスのネットワーク オブジェクトの名前を指定します。
trap | **poll**	（オプション）ホストでトラップの参照（ポーリング）または送信を許可するかどうかを指定します。何も指定されていない場合のデフォルトは **poll** です。同じホスト グループに対して、トラップとポーリングの両方を有効にすることはできません。
udp-port *port*	（オプション）SNMP トラップがデフォルト以外のポートで NMS ホストに送信されるように指定し、NMS ホストの UDP ポート番号を設定します。
user-list *list_name*	ユーザ リストの名前を指定します。
username	ユーザの名前を指定します。
version {**1** | **2c** | **3**}	（オプション）トラップの送信に使用するために、SNMP 通知バージョンをバージョン 1、2c、または 3 に設定します。

デフォルト

デフォルトは poll です。

デフォルトの UDP ポートは 162 です。

デフォルトのバージョンは 1 です。

SNMP トラップはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホスト名または IP アドレスの範囲を使用してホストを定義できます。ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザを関連付けることができます。

[**trap** | **poll**] を指定していない場合のデフォルトは **poll** です。このコマンドでは、同じホスト グループに対して trap と polling の両方を有効にできないことに注意してください。これが必要な場合、該当するホストに対して **snmp-server host** コマンドを使用することを推奨します。

トラップの送信に SNMP 通知バージョン 1 または 2c を使用する場合、1 人のユーザとネットワーク オブジェクトを関連付けることができます。トラップの送信に SNMP 通知バージョン 3 を使用する場合、1 人のユーザまたはユーザ グループをネットワーク オブジェクトに関連付けることができます。ユーザ グループを作成するには、**snmp-server user-list** コマンドを使用します。ユーザは、グループ設定に属する場合があります。

SNMP バージョン 3 を使用する場合、ユーザ名と SNMP ホストを関連付ける必要があります。

IPv4 のみをサポートします。

例

次に、SNMP 通知バージョン 1 を使用して 1 人のユーザとネットワーク オブジェクトを関連付ける例を示します。

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
```

次に、SNMP 通知バージョン 2c を使用して 1 人のユーザとネットワーク オブジェクトを関連付ける例を示します。

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
```

次に、SNMP 通知バージョン 3 を使用して 1 人のユーザとネットワーク オブジェクトを関連付ける例を示します。

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
```

次に、SNMP 通知バージョン 3 を使用してユーザ リストとネットワーク オブジェクトを関連付ける例を示します。

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

関連コマンド

コマンド	説明
clear configure snmp-server host-group	すべての SNMP ホスト グループ設定をクリアします。
show running-config snmp-server host-group	実行コンフィギュレーションから SNMP サーバ ホスト グループ設定をフィルタリングします。
snmp-server host	SNMP ホスト アドレスを設定します。

snmp-server listen-port

SNMP 要求のリスニング ポートを設定するには、グローバル コンフィギュレーション モードで **snmp-server listen-port** コマンドを使用します。デフォルトのポートに戻すには、このコマンドの **no** 形式を使用します。

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

構文の説明

lport	着信要求が受け入れられるポート[1]。

1. **snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。

デフォルト

デフォルト ポートは 161 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

警告 **UDP ポート** *port* **は、別の機能によって使用されています。異なるポートを使用するように snmp-server listen-port コマンドが設定されるまで、デバイスへの SNMP 要求は失敗します。**

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

例

次に、リスニング ポートを 192 に設定する例を示します。

```
ciscoasa(config)# snmp-server listen-port 192
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server location

SNMP の ASA の場所を設定するには、グローバル コンフィギュレーション モードで **snmp-server location** コマンドを使用します。場所を削除するには、このコマンドの **no** 形式を使用します。

snmp-server location *text*

no snmp-server location [*text*]

構文の説明

location *text*	セキュリティ アプライアンスの場所を指定します。**location** *text* は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、SNMP の ASA の場所を Building 42、Sector 54 として設定する例を示します。

```
ciscoasa(config)# snmp-server location Building 42, Sector 54
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。

snmp-server user

新しい SNMP ユーザを設定するには、グローバル コンフィギュレーション モードで **snmp-server user** コマンドを使用します。指定した SNMP ユーザを削除するには、このコマンドの **no** 形式を使用します。

snmp-server user *username group-name* {**v3** [**engineID** *engineID*] [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

no snmp-server user *username group-name* {**v3** [**engineID** *engineID*] [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

構文の説明

128	(任意)暗号化について 128 ビット AES アルゴリズムの使用を指定します。
192	(任意)暗号化について 192 ビット AES アルゴリズムの使用を指定します。
256	(任意)暗号化について 256 ビット AES アルゴリズムの使用を指定します。
3des	(任意)暗号化について 168 ビット 3DES アルゴリズムの使用を指定します。
aes	(任意)暗号化について AES アルゴリズムの使用を指定します。
auth	(任意)使用する認証レベルを指定します。
auth-password	(任意)エージェントがホストからパケットを受信できるようにするストリングを指定します。最小の長さは 1 文字、最低 8 文字で英文字と数字を含むものを推奨します。最大長は、64 文字です。プレーン テキストのパスワードか、ローカライズされた MD5 ダイジェストを指定できます。ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイジェストは、aa:bb:cc:dd という形式であることが必要です(aa、bb、cc は 16 進数の値)。ダイジェストは正確に 16 個のオクテットであることが必要です。
des	(任意)暗号化について 56 ビット DES アルゴリズムの使用を指定します。
engineID	(オプション)ユーザの認証と暗号化の情報をローカライズするために使用される ASA のエンジン ID を指定します。engineID 引数には、有効な ASA エンジン ID を指定する必要があります。
encrypted	(任意)パスワードが暗号化された形式で表示されるかどうかを指定します。暗号化されたパスワードは、16 進数の形式である必要があります。
group-name	ユーザが属すグループの名前を指定します。
md5	(任意)HMAC-MD5-96 認証レベルを指定します。
priv	暗号化されたパケット認証を指定します。
priv-password	(任意)プライバシー ユーザ パスワードを示すストリングを指定します。最小の長さは 1 文字、最低 8 文字で英文字と数字を含むものを推奨します。最大長は、64 文字です。プレーン テキストのパスワードか、ローカライズされた MD5 ダイジェストを指定できます。ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイジェストは、aa:bb:cc:dd という形式であることが必要です(aa、bb、cc は 16 進数の値)。ダイジェストは正確に 16 個のオクテットであることが必要です。
sha	(任意)HMAC-SHA-96 認証レベルを指定します。
username	エージェントに接続するホストのユーザ名を指定します。
v3	SNMP バージョン 3 セキュリティ モデルを使用することを指定します。**encrypted**、**priv**、または **auth** キーワードの使用を許可します。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン　SNMP ユーザは、SNMP グループの一部である必要があります。バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定した後、SNMP ホストを設定する必要があります。

(注)　パスワードを忘れた場合は、回復できないため、ユーザを再設定する必要があります。

snmp-server user のコンフィギュレーションがコンソールに表示されるか、ファイル(スタートアップ コンフィギュレーション ファイルなど)に書き込まれる場合、ローカライズされた認証およびプライバシー ダイジェストが常にプレーン テキストのパスワードの代わりに表示されます。この使用法は、RFC 3414、11.2 項によって要求されています。

(注)　3DES または AES アルゴリズムを使用してユーザを設定するには、3DES または AES 機能のライセンスが必要です。

ASA の起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

クラスタリング環境では、クラスタ化されたそれぞれの ASA について手動で SNMPv3 ユーザを更新する必要があります。これを行うには、マスター ユニットに対する **snmp-server user** *username group-name* **v3** コマンドを入力し、ローカライズされていない形式で *priv-password* オプションおよび *auth-password* オプションを指定します。

クラスタリングの複製または設定時に、SNMPv3 ユーザ コマンドが複製されないことを通知するエラー メッセージが表示されます。この場合、SNMPv3 ユーザおよびグループのコマンドをスレーブの ASA に対して個別に設定します。また、複製の実行時に既存の SNMPv3 ユーザおよびグループのコマンドがクリアされない場合にもメッセージが表示されます。この場合は、クラスタのすべてのスレーブに対して SNMPv3 ユーザおよびグループのコマンドを入力します。次に例を示します。

マスター ユニットに対するコマンドで入力したキーがすでにローカライズされている場合:

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a priv aes 256
cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:f6:86:cf:18:c0:f0:47:d6:94:e5:
da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

クラスタ複製時のスレーブ ユニットの場合(**snmp-server user** コマンドが設定にある場合にのみ表示されます):

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

例

次に、ASA で SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する例を示します。

```
ciscoasa(config)# snmp-server group engineering v3 auth
ciscoasa(config)# snmp-server user engineering v3 auth sha mypassword
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server group	新しい SNMP グループを作成します。
snmp-server host	SNMP ホスト アドレスを設定します。

snmp-server user-list

指定されたユーザ グループを使用して SNMP ユーザ リストを設定するには、グローバル コンフィギュレーション モードで **snmp-server user-list** コマンドを使用します。指定した SNMP ユーザ リストを削除するには、このコマンドの **no** 形式を使用します。

snmp-server user-list *list_name* **username** *user_name*

no snmp-server user-list *list_name* **username** *user_name*

構文の説明

list_name	ユーザ リスト名（最長 33 文字）を指定します。
username *user_name*	ユーザ リストに設定できるユーザを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

snmp-server user *username* コマンドを使用して、ユーザ リストのユーザを設定します。ユーザ リストには複数のユーザを含める必要があり、ホスト名または IP アドレスの範囲に関連付けることができます。

例

次に、engineering という名前のユーザ リストのユーザ グループを作成する例を示します。

```
ciscoasa(config)# snmp-server user-list engineering username user1
ciscoasa(config)# snmp-server user-list engineering username user2
ciscoasa(config)# snmp-server user-list engineering username user3
```

関連コマンド

コマンド	説明
show running-config snmp-server user-list	実行コンフィギュレーションから SNMP ユーザ リストの設定をフィルタリングします。
clear snmp-server user-list	SNMP ユーザ リストの設定をクリアします。

sntp address

DHCPv6 サーバを設定するときに、Simple Network Time Protocol（SNTP）サーバ IP アドレスをステートレス アドレス自動設定（SLAAC）クライアントに提供するには、ipv6 dhcp プール コンフィギュレーション モードで **sntp address** コマンドを使用します。SNTP サーバを削除するには、このコマンドの **no** 形式を使用します。

sntp address *sntp_ipv6_address*

no sntp address *sntp_ipv6_address*

構文の説明

sntp_ipv6_address	SNTP サーバの IPv6 アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、SNTP サーバを含め、**ipv6 dhcp プール**内の情報を提供するように ASA を設定できます。ASA は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。DHCPv6 ステートレス サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    dns-server 2001:DB8:1::1
    sntp address 2001:DB8:1::5
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    dns-server 2001:DB8:1::1
    sntp address 2001:DB8:1::5
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。

コマンド	説明
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。

software authenticity development コマンド～ strip-realm コマンド

software authenticity development

開発キー署名付きイメージのロードをイネーブルまたはディセーブルにするには、パラメータ コンフィギュレーション モードで **software authenticity development** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このオプションは、一度イネーブルにすると、開発キー署名付きイメージのロードをディセーブルにするまで維持されます。

software authenticity development {enable | disable}

構文の説明

disable	開発キー署名付きイメージのロードをディセーブルにします。
enable	開発キー署名付きイメージのロードをイネーブルにします。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、開発キー署名付きシグニチャのロードをイネーブルにする例を示します。

```
ciscoasa(config)# software authenticity development enable
ciscoasa(config)# show software authenticity development
Loading of development images is enabled
ciscoasa(config)#
```

次に、開発キー署名付きイメージのロードをディセーブルにする例を示します。

```
ciscoasa(config)# software authenticity development disable
ciscoasa(config)# show software authenticity development
Loading of development images is disabled
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show software authenticity keys	開発キーを表示します。
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。
software authenticity key add special	SPI フラッシュに新しい開発キーを追加します。
software authenticity key revoke special	SPI フラッシュから古い開発キーを削除します。

software authenticity key add special

SPI フラッシュに新しい開発キーを追加するには、パラメータ コンフィギュレーション モードで **software authenticity key add special** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。

software authenticity key add special

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、SPI フラッシュに新しい開発キーを追加する例を示します。

```
ciscoasa(config)# software authenticity key add special
Writing the key to Primary...Success
Writing the key to Backup...Success
Done!
```

次に、SPR フラッシュに新しい開発イメージを追加しようとしたときに、すでに存在した場合の処理を示します。

```
ciscoasa(config)# software authenticity key add special
Duplicate key found in Primary...Skipping key write
Duplicate key found in Backup...Skipping key write
Done!
```

関連コマンド

コマンド	説明
software authenticity key revoke special	SPI フラッシュから古い開発キーを削除します。
show software authenticity keys	SPI フラッシュの開発キーを表示します。
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。

software authenticity key revoke special

SPI フラッシュから古い開発キーを削除するには、パラメータ コンフィギュレーション モードで **software authenticity key revoke special** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。

software authenticity key revoke special

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、SPI フラッシュから開発キーを削除する例を示します。

```
ciscoasa(config)# software authenticity key revoke special
Revoking the key with version A...Success
Revoking the key with version A...Success
Done!
```

関連コマンド

コマンド	説明
software authenticity key add special	SPI フラッシュに新しい開発キーを追加します。
show software authenticity keys	SPI フラッシュの開発キーを表示します。

コマンド	説明
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。

software-version

サーバまたはエンドポイントのソフトウェア バージョンを表示するサーバおよびユーザ エージェント ヘッダー フィールドを識別するには、パラメータ コンフィギュレーション モードで **software-version** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

software-version action {mask | log} [log]

no software-version action {mask | log} [log]

構文の説明

ログ	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。
mask	SIP メッセージ内のソフトウェア バージョンをマスクします。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップでソフトウェア バージョンを識別する例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# software-version action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

source-interface

VXLAN VTEP インターフェイスの送信元インターフェイス名を指定するには、nve コンフィギュレーション モードで **source-interface** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

source-interface *interface_name*

no source-interface *interface_name*

構文の説明

interface_name	VTEP 送信元インターフェイス名を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Nve コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

VTEP 送信元インターフェイスは、ASA の通常のインターフェイス（物理、冗長、EtherChannel、または VLAN）であり、すべての VNI インターフェイスに関連付けます。ASA/セキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティ ポリシーを適用できます。ただし、VXLAN トラフィックの場合は、すべてのセキュリティ ポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレント ファイアウォール モードでは、VTEP 送信元インターフェイスは、BVI の一部ではないため、その IP アドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

（注） 送信元インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレス テーブル）を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

speed

銅線（RJ-45）イーサネット インターフェイスの速度を設定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。速度設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

no speed [**auto** | **10** | **100** | **1000** | **nonegotiate**]

構文の説明

10	速度を 10BASE-T に設定します。
100	速度を 100BASE-T に設定します。
1000	速度を 1000BASE-T に設定します。銅線ギガビット イーサネット専用。
[auto]	速度を自動検出します。
nonegotiate	ファイバ インターフェイスの場合は、速度を 1000 Mbps に設定し、リンク パラメータをネゴシエートしません。ファイバ インターフェイスに対して使用できる設定は、このコマンドとこのコマンドの **no** 形式だけです。値を **no speed nonegotiate**（デフォルト）に設定すると、インターフェイスでリンク ネゴシエーションがイネーブルになり、フロー制御パラメータとリモート障害情報が交換されます。

デフォルト

銅線インターフェイスの場合、デフォルトは **speed auto** です。

ファイバ インターフェイスの場合、デフォルトは **no speed nonegotiate** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。
9.14(1)	Firepower 1000 および 2100 の 1GB ファイバインターフェイスで、**speed nonegotiate** コマンドを使用して速度の自動ネゴシエーションを無効にできるようになりました。

使用上のガイドライン

速度は物理インターフェイスだけで設定します。

ネットワークで自動検出がサポートされていない場合は、速度を特定の値に設定します。

ASA 5500 シリーズの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

PoE ポートで速度を **auto** 以外に設定する場合（可能な場合）、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコ ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

（注） ファイバインターフェイス搭載の ASA 5500-X または ASA 5585-X に対して **speed** コマンドを設定しないでください。設定すると、リンク障害が発生します。

例

次に、速度を 1000BASE-T に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
duplex	デュプレックス モードを設定します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイス コンフィギュレーションを表示します。

spf-interval

最短パス優先（SPF）計算の IS-IS スロットリングをカスタマイズするには、ルータ isis コンフィギュレーション モードで **spf-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

spf-interval [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]

no spf-interval [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]

構文の説明

level-1	（任意）レベル 1 エリアだけに間隔を適用します。
level-2	（任意）レベル 2 エリアだけに間隔を適用します。
spf-max-wait	連続する 2 つの SPF 計算の最大間隔（秒単位）を示します。指定できる範囲は 1 ～ 120 秒です。デフォルトは 10 秒です。
spf-initial-wait	（任意）トポロジが変更された後の初期 SPF 計算遅延（ミリ秒単位）を示します。有効な範囲は 1 ～ 120000 ミリ秒です。デフォルト値は 5500 ミリ秒（5.5 秒）です。
spf-second-wait	（任意）最初と 2 番目の SPF 計算の間のホールド タイム（ミリ秒単位）を示します。有効な範囲は 1 ～ 120000 ミリ秒です。デフォルト値は 5500 ミリ秒（5.5 秒）です。

コマンド デフォルト

spf-max-wait：10 秒

spf-initial-wait：5500 ミリ秒

spf-second-wait：5500 ミリ秒

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

SPF 計算が実行されるのは、トポロジが変更されたときだけです。外部ルートが変更された場合は実行されません。

spf-interval コマンドは、ソフトウェアが SPF 計算を実行する頻度を制御します。SPF 計算は、プロセッサに高い負荷を与えます。そのため、特にエリアが広くトポロジが頻繁に変わる場合には、計算を実行する頻度を制限することが有効です。SPF 間隔を大きくすると、ルータのプロセッサ負荷が軽減されますが、コンバージェンスの速度が低下する可能性があります。

次の説明を参照して、このコマンドのデフォルト値を変更するかどうか決定する際の参考にしてください。

- *spf-initial-wait* 引数は、トポロジが変更されてから最初の SPF 計算までの初期の待機時間（ミリ秒単位）を示します。
- *spf-second-wait* 引数は、最初と 2 番目の SPF 計算の間の間隔（ミリ秒単位）を示します。
- 後続の各待機間隔は、指定された *spf-max-wait* 間隔に達するまで、前の待機間隔の 2 倍の長さになります。SPF 計算は、最初と 2 番目の間隔の後にスロットルされるか、スローダウンします。*spf-max-wait* 間隔に達すると、待機間隔はネットワークが安定するまでこの間隔に維持されます。
- ネットワークが安定して、*spf-max-wait* 間隔の 2 倍の時間内にトリガーがない場合は、高速動作（初期の待機時間）に戻ります。

SPF スロットリングはダンプニング メカニズムではありません。つまり、SPF スロットリングは SPF 計算を阻止せず、ルート、インターフェイス、またはルータをダウンとしてマークしません。SPF スロットリングは、SPF 計算の間の間隔を単に長くするに過ぎません。

例

次に、SPF 計算、部分的なルート計算（PRC）、およびリンクステート パケット（LSP）生成の間隔を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# spf-interval 5 10 20
ciscoasa(config-router)# prc-interval 5 10 20
ciscoasa(config-router)# lsp-gen-interval 2 50 100
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。

コマンド	説明
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。

コマンド	説明
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
summary-address	IS-IS の集約アドレスを作成します。

split-dns

スプリット トンネルを介して解決されるドメインのリストを入力するには、グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ドメインのリストをすべて削除するには、**no split-dns** コマンドを引数なしで使用します。これにより、**split-dns none** コマンドを発行して作成されたヌル リストを含め、設定されているスプリット トンネリング ドメインのリストはすべて削除されます。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルトのグループ ポリシー内に存在するリストを継承します。このようなスプリット トンネリング ドメインのリストをユーザが継承しないようにするには、**split-dns none** コマンドを使用します。

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

構文の説明

value *domain-name*	スプリット トンネルを介して ASA が解決するドメイン名を指定します。
none	スプリット DNS リストがないことを指定します。スプリット DNS リストをヌル値で設定して、スプリット DNS リストを拒否します。デフォルトのグループ ポリシーまたは指定したグループ ポリシーのスプリット DNS リストを継承しません。

デフォルト

スプリット DNS はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ドメインのリスト内の各エントリを区切るには、単一のスペースを使用します。エントリ数に制限はありませんが、ストリング全体の長さは 255 文字以下にします。英数字、ハイフン(-)、およびピリオド(.)のみを使用できます。

no split-dns コマンドを引数なしで使用すると、**split-dns none** コマンドを発行して作成したヌル値を含め、現在の値はすべて削除されます。

バージョン 3.0.4235 から、AnyConnect セキュア モビリティ クライアントは Windows プラットフォーム向けのトゥルー スプリット DNS 機能をサポートしています。

例

次に、FirstGroup という名前のグループ ポリシーに対してスプリット トンネリングを介して解決されるドメイン Domain1、Domain2、Domain3、および Domain4 を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドが除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークを区別するために、ASA が使用するアクセス リストを指定します。
split-tunnel-policy	IPsec クライアントが、条件に応じてパケットを暗号化形式で IPsec トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようにします。

split-horizon

EIGRP スプリット ホライズンを再度イネーブルにするには、インターフェイス コンフィギュレーション モードで **split-horizon** コマンドを使用します。EIGRP スプリット ホライズンをディセーブルにするには、このコマンドの **no** 形式を使用します。

split-horizon eigrp *as-number*

no split-horizon eigrp *as-number*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。

デフォルト

split-horizon コマンドはイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

X.25 パケットスイッチド ネットワーク上のリンクを含むネットワークでは、**neighbor** コマンドを使用してスプリット ホライズン機能を無効にすることができます。代わりに、コンフィギュレーションで **no split-horizon eigrp** コマンドを明示的に指定することもできます。ただし、その場合、そのネットワーク上の関連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバに対して、同様にスプリット ホライズンをディセーブルにする必要があります。

通常、スプリット ホライズンのデフォルトの状態は、ルートを適切にアドバタイズするために変更することがアプリケーションにおいて必要となる場合を除き、変更しないことを推奨します。シリアル インターフェイスでスプリット ホライズンがディセーブルであり、そのインターフェイスがパケットスイッチド ネットワークに接続されている場合、そのネットワーク上の関連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバに対して、スプリット ホライズンをディセーブルにする必要があります。

例

次に、インターフェイス Ethernet0/0 で EIGRP スプリット ホライズンをディセーブルにする例を示します。

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# no split-horizon eigrp 100
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

split-tunnel-all-dns

AnyConnect セキュア モビリティ クライアントが VPN トンネルを経由するすべての DNS アドレスを解決できるようにするには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-all-dns** コマンドを使用します。

実行コンフィギュレーションからこのコマンドを削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーの値を継承できます。

split-tunnel-all-dns {**disable** | **enable**}

no split-tunnel-all-dns [{**disable** | **enable**}]

構文の説明

disable（デフォルト）	AnyConnect クライアントは、スプリット トンネル ポリシーに従ってトンネル経由で DNS クエリーを送信します。ポリシーは、すべてのネットワークをトンネリング、ネットワーク リストで指定されたネットワークをトンネリング、ネットワーク リストで指定されたネットワークを除外、のいずれかです。
enable	AnyConnect クライアントは、VPN トンネルを経由するすべての DNS アドレスを解決します。

デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(5)	このコマンドが追加されました。

使用上のガイドライン

split-tunnel-all-dns enable コマンドは、SSL プロトコルまたは IPsec/IKEv2 プロトコルを使用する VPN 接続に適用され、AnyConnect クライアントに対して VPN トンネルを経由するすべての DNS アドレスを解決するように指示します。DNS 解決に失敗すると、アドレスは未解決のまま残ります。AnyConnect Client は、パブリック DNS サーバ経由でアドレスを解決しようとはしません。

デフォルトでは、この機能はディセーブルになっています。クライアントは、スプリット トンネル ポリシーに従ってトンネル経由で DNS クエリーを送信します。ポリシーは、すべてのネットワークをトンネリング、ネットワーク リストで指定されたネットワークをトンネリング、またはネットワーク リストで指定されたネットワークを除外です。

例

次に、AnyConnect クライアントが VPN トンネルを経由するすべての DNS クエリーを解決できるように ASA を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-all-dns enable
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドが省略された DNS クエリーに対してレガシー IPsec（IKEv1）VPN クライアントまたは AnyConnect VPN Client（SSL）が使用するデフォルトのドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、ASA が使用するアクセス リストを指定します。
split-tunnel-policy	レガシー VPN クライアント（IPsec/IKEv1）または AnyConnect VPN クライアント（SSL）が、条件に応じてパケットを暗号化形式でトンネルを経由して転送したり、クリア テキスト形式でネットワーク インターフェイスに転送したりできるようにします。

split-tunnel-network-list

スプリット トンネリングのネットワーク リストを作成するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用します。ネットワーク リストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ネットワーク リストをすべて削除するには、**no split-tunnel-network-list** コマンドを引数なしで使用します。これにより、**split-tunnel-network-list none** コマンドを発行して作成されたヌル リストを含め、設定されているネットワーク リストはすべて削除されます。

スプリット トンネリング ネットワーク リストがない場合、ユーザはデフォルトのグループ ポリシーまたは指定したグループ ポリシー内に存在するネットワーク リストを継承します。このようなネットワーク リストをユーザが継承しないようにするには、**split-tunnel-network-list none** コマンドを使用します。

スプリット トンネリング ネットワーク リストによって、トラフィックがトンネルを通過する必要があるネットワークと、トンネリングを必要としないネットワークが区別されます。

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

構文の説明

none	スプリット トンネリングのネットワーク リストがないことを指定します。ASA によって、すべてのトラフィックがトンネリングされます。 スプリット トンネリング ネットワーク リストをヌル値で設定して、スプリット トンネリングを拒否します。デフォルトのグループ ポリシーまたは指定したグループ ポリシーのデフォルトのスプリット トンネリング ネットワーク リストを継承しません。
value *access-list name*	トンネリングするネットワークまたはトンネリングしないネットワークを列挙するアクセス リストを指定します。

デフォルト

デフォルトでは、スプリット トンネリング ネットワーク リストはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA では、ネットワーク リストに基づいてスプリット トンネリングの判断が行われます。ネットワーク リストは、プライベート ネットワーク上のアドレスのリストで構成される標準 ACL です。

no split-tunnel-network-list コマンドを引数なしで使用すると、**split-tunnel-network-list none** コマンドを発行して作成したヌル値を含め、現在のネットワーク リストはすべて削除されます。

(注) ASA は、200 のスプリット ネットワークをサポートします。

例

次に、FirstGroup という名前のグループ ポリシーに対して FirstList という名前のネットワーク リストを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-network-list FirstList
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
default-domain	ドメイン フィールドが除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-policy	IPSec クライアントが、条件に応じてパケットを暗号化形式で IPSec トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようにします。

split-tunnel-policy

スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを使用します。実行コンフィギュレーションから split-tunnel-policy 属性を削除するには、このコマンドの **no** 形式を使用します。

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no split-tunnel-policy

構文の説明

excludespecified	トラフィックを暗号化しないで送信する先となるネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザにとって役立ちます。
split-tunnel-policy	トラフィックのトンネリングのルールを設定することを指定します。
tunnelall	トラフィックを暗号化しないで送信しないこと、または ASA 以外の宛先に送信しないことを指定します。リモート ユーザは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。
tunnelspecified	指定したネットワークから、または指定したネットワークへのすべてのトラフィックをトンネリングします。このオプションによって、スプリット トンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。その他のすべてのアドレスへのデータは暗号化しないで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

デフォルト

スプリット トンネリングは、デフォルト（**tunnelall**）ではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

スプリット トンネリングは、本来は、セキュリティ機能ではなくトラフィック管理機能です。最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

これにより、別のグループ ポリシーのスプリット トンネリングの値を継承できます。

スプリット トンネリングを使用すると、リモート アクセス VPN クライアントが、条件に応じて、パケットを暗号化形式で IPsec トンネルまたは SSL トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようになります。スプリット トンネリングをイネーブルにすると、宛先が IPSec または SSL VPN トンネル エンドポイントの反対側ではないパケットでは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングは必要なくなります。

例

次に、FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドが除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list none	スプリット トンネリングのアクセス リストがないことを指定します。トラフィックはすべてトンネルを通過します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために、ASA が使用するアクセス リストを指定します。

spoof-server

HTTP プロトコル インスペクションのために、サーバ ヘッダー フィールドをストリングに置き換えるには、パラメータ コンフィギュレーション モードで **spoof-server** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

spoof-server *string*

no spoof-server *string*

構文の説明

string	サーバ ヘッダー フィールドを置き換えるストリング。最大 82 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

WebVPN ストリームは **spoof-server** コマンドの対象になりません。

例

次に、HTTP インスペクション ポリシー マップでサーバ ヘッダー フィールドをあるストリングに置き換える例を示します。

```
ciscoasa(config-pmap-p)# spoof-server string
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

sq-period

NAC フレームワーク セッションで正常に完了したポスチャ検証と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **sq-period** コマンドを使用します。このコマンドを NAC ポリシーから削除するには、このコマンドの **no** 形式を使用します。

sq-period *seconds*

no sq-period [*seconds*]

構文の説明

seconds	正常に完了した各ポスチャ確認の間隔の秒数。指定できる範囲は 30 ～ 1800 です。

デフォルト

デフォルト値は 300 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.3(0)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA では、正常に実行された各ポスチャ検証とステータス クエリー応答の後に、ステータス クエリー タイマーを起動します。このタイマーが切れると、ホスト ポスチャの変化を調べるクエリー（*ステータス クエリー*と呼ばれる）がトリガーされます。

例

次に、ステータス クエリー タイマーの値を 1800 秒に変更する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# sq-period 1800
ciscoasa(config-nac-policy-nac-framework)
```

次に、NAC フレームワーク ポリシーからステータス クエリー タイマーを削除する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# no sq-period
ciscoasa(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
debug eap	NAC フレームワーク メッセージのデバッグのための拡張認証プロトコル イベントのロギングをイネーブルにします。

srv-id

参照 ID オブジェクトに URI ID を設定するには、*ca-reference-identity* モードで **uri-id** コマンドを使用します。URI ID を削除するには、このコマンドの **no** 形式を使用します。最初に、**crypto ca reference-identity** コマンドを入力して参照 ID オブジェクトを設定することで、*ca-reference-identity* モードにアクセスできます。

srv-id *value*

no srv-id *value*

構文の説明

value	各参照 ID の値。
srv-id	RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ca-reference-identity	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

例

次に、syslog サーバの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
crypto ca reference-identity	参照 ID オブジェクトを設定します。
cn-id	参照 ID オブジェクトのコモン ネーム ID を設定します。
dns-id	参照 ID オブジェクトの DNS ドメイン名 ID を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギング サーバを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバを設定します。

ss7 variant

M3UA インスペクション用にネットワーク内で使用されている SS7 バリエーションを特定するには、パラメータ コンフィギュレーション モードで **ss7 variant** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect m3ua** コマンドを入力します。デフォルトの SS7 バリエーションに戻すには、このコマンドの **no** 形式を使用します。

ss7 variant {**ITU** | **ANSI** | **Japan** | **China**}

no ss7 variant {**ITU** | **ANSI** | **Japan** | **China**}

構文の説明

国際電気通信連合（ITU）	ITU のバリエーション。これはデフォルトです。
ANSI	ANSI のバリエーション。
Japan	日本のバリエーション。
中国	中国のバリエーション。

デフォルト

デフォルトは、ITU SS7 バリエーションです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、ネットワーク内で使用されている SS7 バリエーションを特定できます。オプションを設定して、M3UA ポリシーを導入した後は、最初にポリシーを削除しないかぎり、ポリシーを変更することはできません。

バリエーションによって、M3UA メッセージで使用されるポイント コードの形式が決まります。

- ITU: ポイント コードは 14 ビットで 3-8-3 形式です。値の範囲は、[0-7]-[0-255]-[0-7] です。これは、デフォルトの SS7 バリエーションです。
- ANSI: ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。

- Japan：ポイント コードは 16 ビットで 5-4-7 形式です。値の範囲は、[0-31]-[0-15]-[0-127] です。
- China：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。

例

次に、SS7 バリエーションを ITU に設定する例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
match dpc	M3UA 宛先ポイント コードと一致させます。
match opc	M3UA 発信ポイント コードと一致させます。
policy-map type inspect	インスペクション ポリシー マップを作成します。

ssh

ASA に SSH アクセスを追加するには、グローバル コンフィギュレーション モードで **ssh** コマンドを使用します。ASA への SSH アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh {*ip_address mask* | *ipv6_address/prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address/prefix*} *interface*

構文の説明

interface	SSH をイネーブルにする ASA インターフェイス。名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。VPN 管理アクセスのみ（**management-access** コマンドを参照）の場合、名前付き BVI インターフェイスを指定します。
ip_address	ASA への SSH 接続を開始することを認可されるホストまたはネットワークの IPv4 アドレス。
ipv6_address/prefix	ASA への SSH 接続を開始することを認可されるホストまたはネットワークの IPv6 アドレスとプレフィックス。
mask	*ip_address* のネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(2)	**pix** または **asa** ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカル ユーザを定義する必要があります。ローカル ユーザを定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。
8.4(4.1)、9.1(2)	**ssh authentication** コマンドを使用すると、ユーザ単位で、ASA への SSH 接続の公開キー認証を有効にすることができます。
9.1(2)	ASA での SSH サーバの実装が、AES-CTR モードの暗号化をサポートするようになりました。
9.1(7)/9.4(3)/9.5(3)/9.6(1)	**ssh cipher encryption** コマンドおよび **ssh cipher integrity** コマンドを使用して、SSH アクセスの暗号化と整合性の方式を設定できます。
9.6(2)	**ssh authentication** には、**aaa authentication ssh console LOCAL** コマンドが必須です。バージョン 9.6(2) 以降では、パスワードを定義せずに**ユーザ名**を作成できるため、公開キー認証のみが必要となります。
9.7(1)	直接接続された SSH 管理ステーションがある場合、ASA およびホストの /31 サブネットを使用してポイントツーポイント接続を作成できます。
9.6(3)/9.8(1)	SSH 公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。AAA SSH 認証（**aaa authentication ssh console**）を明示的にイネーブルにする必要がなくなりました。ユーザに **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトでイネーブルになります。さらに、明示的に AAA SSH 認証を設定すると、パスワードを持つユーザ名のみにこの認証が適用されます。また、AAA サーバ タイプを使用できます。
9.9(2)	仮想インターフェイスが指定可能になりました。

使用上のガイドライン

ssh *ip_address* コマンドでは、ASA への SSH 接続を開始することを認可されるホストまたはネットワークを指定します。複数の **ssh** コマンドをコンフィギュレーションに含めることができます。

ASA への SSH の使用を開始する前に、**crypto key generate rsa** コマンドを使用してデフォルトの RSA キーを生成する必要があります。

また、ASA インターフェイスに SSH アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。

ASA への通過ルートとなるインターフェイス以外のインターフェイスへの SSH アクセスはサポートされません。たとえば、SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです（**management-access** コマンドを参照）。

ASA は、コンテキスト/単一のモードあたり最大 5 つの同時 SSH 接続と、すべてのコンテキストにまたがり分散された最大 100 の接続を許容します。

ASA は SSH バージョン 2 で提供されている SSH リモート シェル機能をサポートし、DES 暗号方式および 3DES 暗号方式をサポートします。

次の SSH バージョン 2 機能は、ASA でサポートされていません。

- X11 転送。
- ポート フォワーディング。
- SFTP サポート。
- Kerberos と AFS のチケット引き渡し
- データ圧縮

ユーザ名およびパスワードとともに SSH を使用するには、**aaa authentication ssh console LOCAL** コマンドを使用して AAA 認証を設定し、**username** コマンドを入力してローカル ユーザを定義する必要があります。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

ローカル **ユーザ名**および公開キー認証とともに SSH を使用するには、**ssh authentication** コマンドを設定します。ローカル データベースのみがサポートされます。

バージョン 9.6(2) および 9.7(1) では、**ssh authentication** には **aaa authentication ssh console LOCAL** コマンドが必要です。バージョン 9.6(2) 以降では、パスワードを定義せずに**ユーザ名**を作成できるため、公開キー認証のみが必要となります。

(注) パスワードとともにユーザ名を作成する必要を回避するために、**username** コマンドの **nopassword** オプションを使用しないでください。**nopassword** オプションでは*任意の*パスワードを入力できます。「パスワードなし」ではありません。**aaa** コマンドを設定する場合、**nopassword** オプションによってセキュリティ問題が生じます。

9.6(1) 以前および 9.6(3)/9.8(1) 以降では、**aaa authentication ssh console LOCAL** コマンドを設定する必要はありません。このコマンドは、パスワードを持つユーザのみに適用されます。また、LOCAL だけでなく、任意のサーバ タイプを指定できます。たとえば、一部のユーザはローカル データベースを使用して公開キー認証を使用し、他のユーザは RADIUS でパスワードを使用することができます。**aaa authentication ssh console LOCAL** コマンドを設定すると、**username** パスワードと秘密キーのうちのどちらをログインに使用するかを選択できます。

例

次の例は、RSA キーを生成し、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASA にアクセスする方法を示しています。

```
ciscoasa(config)# crypto key generate rsa modulus 1024
ciscoasa(config)# write memory
ciscoasa(config)# aaa authentication ssh console LOCAL

WARNING: local database is empty! Use 'username' command to define local users.

ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
ciscoasa(config)# ssh timeout 30
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
crypto key generate rsa	アイデンティティ証明書用の RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh scopy enable	ASA でセキュア コピー サーバをイネーブルにします。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、ASA を制限します。

ssh authentication

SSH 公開キー認証をユーザ単位で有効にするには、ユーザ名属性モードで **ssh authentication** コマンドを使用します。公開キー認証をユーザ単位でディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh authentication {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

no ssh authentication {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

構文の説明

hashed	**show running-config username** コマンドを使用して ASA 上でキーを表示した場合、キーは、SHA-256 ハッシュを使用して暗号化されます。キーを **pkf** として入力した場合でも、ASA はキーをハッシュし、ハッシュ化された **publickey** として表示します。**show** の出力からキーをコピーする必要がある場合、**hashed** キーワードを使って、**publickey** タイプを指定します。
キー	*key* 引数の値は次のいずれかになります。 • *key* 引数が指定され、ハッシュされたタグが指定されていない場合、キーの値は、SSH-RSA の未処理キーを生成することのできる SSH キー生成ソフトウェアによって生成される Base 64 で符号化された公開キーである必要があります(つまり、証明書は使用しません)。Base 64 エンコード公開キーを送信すると、そのキーは SHA-256 によりハッシュ化され、それ以降のすべての比較では対応する 32 バイト ハッシュが使用されます。 • *key* 引数が指定され、ハッシュされたタグを指定した場合は、キーの値は、SHA-256 で事前にハッシュされている必要があります。長さは 32 バイトで、各バイトはコロンで区切られている必要があります(解析のため)。
nointeractive	**nointeractive** オプションは、SSH 公開キー ファイル形式のキーをインポートするときにすべてのプロンプトを抑制します。この非インタラクティブ データ入力モードは ASDM での使用のみを目的としています。
pkf	**pkf** キーの場合、PKF でフォーマットされたキーを最大 4096 ビット貼り付けるよう求められます。Base64 形式では大きすぎてインラインで貼り付けることができないキーにはこのフォーマットを使用します。たとえば、ssh keygen を使って4096 ビットのキーを生成してから PKF に変換し、そのキーに対して **pkf** キーワードが求められるようにすることができます。 (注) フェールオーバーで **pkf** オプションを使用できますが、PKF キーは、スタンバイ システムに自動的に複製されません。PKF キーを同期するには、**write standby** コマンドを入力する必要があります。
publickey	**publickey** の場合、*key* は Base64 でエンコードされた公開キーです。SSH-RSA raw キー(証明書なし)を生成可能な任意の SSH キー生成ソフトウェア(ssh keygen など)を使用して、キーを生成できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ名属性	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(4.1)、9.1(2)	このコマンドが追加されました。 *この機能は、8.5 (1)、8.6 (1)、8.7 (1)、9.0 (1)、9.0(2)、9.1(1) では、利用できません。*
9.1(2)	**pkf** キーワードと最大 4096 ビットのキーのサポートが追加されました。
9.6(2)	**ssh authentication** には、**aaa authentication ssh console LOCAL** コマンドが必須です。バージョン 9.6(2) 以降では、パスワードを定義せずに**ユーザ名**を作成できるため、公開キー認証のみが必要となります。
9.6(3)/9.8(1)	SSH 公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。AAA SSH 認証（**aaa authentication ssh console**）を明示的にイネーブルにする必要がなくなりました。ユーザに **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトでイネーブルになります。さらに、明示的に AAA SSH 認証を設定すると、パスワードを持つユーザ名のみにこの認証が適用されます。また、AAA サーバ タイプを使用できます。

使用上のガイドライン　ローカル **ユーザ名**の場合、パスワード認証の代わりに公開キー認証を有効にすることができます。SSH-RSA raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、公開キー/秘密キーのペアを生成できます。**ssh authentication** コマンドを使用して、ASA で公開キーを入力します。その後、SSH クライアントは秘密キー（およびキー ペアを作成するために使用したパスフレーズ）を使用して ASA に接続します。

ローカル データベースのみがサポートされます。

設定を保存すると、ハッシュされたキー値はコンフィギュレーションに保存され、ASA のリブート時に使用されます。

バージョン 9.6(2) および 9.7(1) では、**ssh authentication** には **aaa authentication ssh console LOCAL** コマンドが必要です。バージョン 9.6(2) 以降では、パスワードを定義せずに**ユーザ名**を作成できるため、公開キー認証のみが必要となります。

（注）　パスワードとともにユーザ名を作成する必要を回避するために、**username** コマンドの **nopassword** オプションを使用しないでください。**nopassword** オプションでは*任意の*パスワードを入力できます。「パスワードなし」ではありません。**aaa** コマンドを設定する場合、**nopassword** オプションによってセキュリティ問題が生じます。

9.6(1) 以前および 9.6(3)/9.8(1) 以降では、**aaa authentication ssh console LOCAL** コマンドを設定する必要はありません。このコマンドは、パスワードを持つユーザのみに適用されます。また、LOCAL だけでなく、任意のサーバ タイプを指定できます。たとえば、一部のユーザはローカル データベースを使用して公開キー認証を使用し、他のユーザは RADIUS でパスワードを使用することができます。**aaa authentication ssh console LOCAL** コマンドを設定すると、**username** パスワードと秘密キーのうちのどちらをログインに使用するかを選択できます。

例

次に、PKF 形式のキーを使用して認証する例を示します。

```
ciscoasa(config)# crypto key generate rsa modulus 1024
ciscoasa(config)# write memory
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# username exampleuser1 attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+561+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config-username)# aaa authentication ssh console LOCAL
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、ASA を制限します。

ssh cipher encryption

SSH アクセスの設定時に、暗号化および整合性のアルゴリズムを選択できます。SSH 暗号の暗号化アルゴリズムを綿密に制御するには、グローバル コンフィギュレーション モードで **ssh cipher encryption** コマンドを使用します。アルゴリズムの特定のセットに対応する定義済みのレベルを利用できます。また、複数のアルゴリズムをコロンで区切って指定することで、カスタム リストを定義できます。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

ssh cipher encryption {**all** | **fips** | **high** | **low** | **medium** | **custom** *encryption_1*[**:***encryption_2*[**:***...encryption_n*]]}

no ssh cipher encryption [**all** | **fips** | **high** | **low** | **medium** | **custom** *encryption_1*[**:***encryption_2*[**:***...encryption_n*]]]

構文の説明

all	すべての暗号化アルゴリズムを受け入れるように指定します。
custom *encryption_1*[**:***encryption_2*[**:***...encryption_n*]]	暗号化アルゴリズムのカスタム セットを指定します。**show ssh ciphers** コマンドを入力すると、使用可能なすべての暗号化アルゴリズムを表示できます。次に例を示します。 **custom 3des-cbc:aes192-cbc:aes256-ctr**
fips	FIPS 準拠の暗号化アルゴリズムのみを指定します。
high	高強度の暗号化アルゴリズムのみを指定します。
low	低、中、および高強度の暗号化アルゴリズムを指定します。
medium	中および高強度の暗号化アルゴリズムを指定します。

コマンド デフォルト

medium がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(7)/9.4(3)/9.5(3)/9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**ssh cipher integrity** コマンドと一緒に使用されます。暗号化アルゴリズムについては、次の値を指定できます。

- all：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- fips：aes128-cbc、aes256-cbc
- high：aes256-cbc、aes256-ctr
- low：3des-cbc、aes128-cbc、aes192-cbc、aes256-cbc、aes128-ctr、aes192-ctr、aes256-ctr
- medium：3des-cbc、aes128-cbc、aes192-cbc、aes256-cbc、aes128-ctr、aes192-ctr、aes256-ctr

（注） FIPS モードが有効な場合は、FIPS 暗号化および整合性アルゴリズムのみが許可されます。

オプションで、アルゴリズムの一部を選択解除できます。FIPS モードが有効な場合、現在設定されているアルゴリズムと FIPS 準拠のアルゴリズムの共通部分が計算されます。NULL 以外の場合に、結果の構成が使用されます。NULL の場合は、デフォルトの FIPS 準拠のアルゴリズムが使用されます。

セキュア コピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。medium の暗号セットを選択した場合、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式を変更するには、たとえば、**ssh cipher encryption custom aes128-cbc** などの **ssh cipher encryption** コマンドを使用します。

例

次に、いくつかのカスタム SSH 暗号化アルゴリズムの構成の例を示します。

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

関連コマンド

コマンド	説明
show ssh	設定されている暗号方式を表示します。
show ssh ciphers	使用可能な暗号アルゴリズムを表示します。
ssh cipher integrity	設定されている SSH 暗号の整合性アルゴリズムを指定します。

ssh cipher integrity

SSH アクセスの設定時に、暗号化および整合性方式のモードを選択できます。SSH 暗号の整合性アルゴリズムを綿密に制御するには、グローバル コンフィギュレーション モードで **ssh cipher integrity** コマンドを使用します。アルゴリズムの特定のセットに対応する定義済みのレベルを利用できます。また、コロンで区切って複数のアルゴリズムを指定して、カスタム リストを定義できます。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

ssh cipher integrity {**all** | **fips** | **high** | **low** | **medium** | **custom** *algorithm_1*[**:***algorithm_2*[**:***...algorithm_n*]]}

no ssh cipher integrity [**all** | **fips** | **high** | **low** | **medium** | **custom** *algorithm_1*[**:***algorithm_2*[**:***...algorithm_n*]]]

構文の説明

all	すべての整合性アルゴリズムを受け入れるように指定します。
custom *algorithm_1*[**:***algorithm_2*[**:***...algorithm_n*]]	整合性アルゴリズムのカスタム セットを指定します。**show ssh ciphers** コマンドを入力すると、使用可能なすべての整合性アルゴリズムを表示できます。次に例を示します。 **custom hmac-sha1:hmac-sha1-96:hmac-md5-96**
fips	FIPS 準拠の整合性アルゴリズムを指定します。
high	高強度の整合性アルゴリズムのみを指定します。
low	低、中、および高強度の整合性アルゴリズムを指定します。
medium	中および高強度の整合性アルゴリズムを指定します。

コマンド デフォルト

(9.12 以降) High がデフォルトです。

(9.10 以前) Medium がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(7)/9.4(3)/9.5(3)/9.6(1)	このコマンドが追加されました。
9.12(1)	HMAC-SHA256 整合性暗号のサポートが追加されました。デフォルトは、高セキュリティの暗号セット（hmac-sha1 および hmac-sha2-256）になりました。以前のデフォルトは中程度のセットでした。
9.13(1)	次の整合性アルゴリズムの値は、安全ではないと見なされ、廃止されます。 • all：hmac-sha1-96、hmac-md5、hmac-md5-96、hmac-sha2-256 • low：hmac-sha1-96、hmac-md5、hmac-md5-96、hmac-sha2-256 • medium：hmac-sha1-96 上記の値は、以降のリリースから削除されます。

使用上のガイドライン

このコマンドは、**ssh cipher encryption** コマンドと一緒に使用されます。整合性アルゴリズムについては、次の値を指定できます。

- all：hmac-sha1、hmac-sha1-96（廃止）、hmac-md5（廃止）、hmac-md5-96（廃止）、hmac-sha2-256（廃止）
- fips：hmac-sha1, hmac-sha2-256
- high：hmac-sha1, hmac-sha2-256
- low：hmac-sha1、hmac-sha1-96（廃止）、hmac-md5（廃止）、hmac-md5-96（廃止）、hmac-sha2-256（廃止）
- medium：hmac-sha1、hmac-sha1-96（廃止）、hmac-md5、hmac-md5-96、hmac-sha2-256

（注） FIPS モードが有効な場合は、FIPS 暗号化および整合性アルゴリズムのみが許可されます。

オプションで、アルゴリズムの一部を選択解除できます。FIPS モードが有効な場合、現在設定されているアルゴリズムと FIPS 準拠のアルゴリズムの共通部分が計算されます。NULL 以外の場合に、結果の構成が使用されます。NULL の場合は、デフォルトの FIPS 準拠のアルゴリズムが使用されます。

例

次に、いくつかのカスタム SSH 整合性アルゴリズムの構成の例を示します。

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

関連コマンド

コマンド	説明
show ssh	設定されている暗号方式を表示します。
show ssh ciphers	使用可能な暗号アルゴリズムを表示します。
ssh cipher encryption	設定されている SSH 暗号の暗号化アルゴリズムを指定します。

ssh disconnect

アクティブな SSH セッションを切断するには、特権 EXEC モードで **ssh disconnect** コマンドを使用します。

ssh disconnect *session_id*

構文の説明

session_id	ID 番号で指定した SSH セッションを切断します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

セッション ID を指定する必要があります。切断する SSH セッションの ID を取得するには、**show ssh sessions** コマンドを使用します。

例

次に、切断される SSH セッションの例を示します。

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
ciscoasa# ssh disconnect 2
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

関連コマンド

コマンド	説明
show ssh sessions	ASA とのアクティブ SSH セッションに関する情報を表示します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

ssh key-exchange

SSH キー交換方式を設定するには、グローバル コンフィギュレーション モードで **ssh key-exchange** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

ssh key-exchange group {**dh-group1-sha1** | **dh-group14-sha1** | **dh-group14-sha256**}

no ssh key-exchange

構文の説明

dh-group1-sha1	キー交換に DH グループ 1 SHA1 を使用します。
dh-group14-sha1	キー交換に DH グループ 14 SHA1 を使用します。
dh-group14-sha256	キー交換に DH グループ 14 SHA256 を使用します。
group	使用する DH グループを指定します。

デフォルト

(9.12 以降)デフォルトでは、DH Group 14 SHA256 のキー交換方式が使用されます。

(9.10 以前)デフォルトでは、DH Group 1 SHA1 のキー交換方式が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応(管理コンテキストのみ)	—

コマンド履歴

リリース	変更内容
8.4(4.1)、9.1(2)	このコマンドが追加されました。 この機能は、8.5(1)、8.6(1)、8.7(1)、9.0(1)、9.0(2)、9.1(1) では、利用できません。
9.12(1)	Diffie-Hellman グループ 14 SHA256 キー交換が追加され、デフォルトになっています。
9.12(2)	SSH キー交換モードの設定が、管理コンテキストに限定されました。
9.13(1)	dh-group1-sha1- Diffie-Hellman group 2 コマンド オプションは廃止され、以降のリリースで削除されました。

使用上のガイドライン

Diffie-Hellman（DH）キー交換は、いずれかの当事者単独では決定できない共有秘密を提供します。キー交換を署名およびホスト キーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

管理コンテキストでは SSH キー交換を設定する必要があります。この設定は、他のすべてのコンテキストによって継承されます。

例

次に、DH グループ 14 SHA1 のキー交換方式を使用してキーを交換する例を示します。

```
ciscoasa(config)# ssh key-exchange dh-group-14-sha1
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
crypto key generate rsa	アイデンティティ証明書用の RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh scopy enable	ASA でセキュア コピー サーバをイネーブルにします。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、ASA を制限します。

ssh pubkey-chain

オンボードのセキュア コピー（SCP）クライアントの SSH サーバおよびそのキーを ASA データベースに対して手動で追加または削除するには、グローバル コンフィギュレーション モードで **ssh pubkey-chain** コマンドを使用します。すべてのホスト キーを削除するには、このコマンドの **no** 形式を使用します。単一のサーバ キーだけを削除するには、**server** コマンドを参照してください。

ssh pubkey-chain

no ssh pubkey-chain

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

オンボードの SCP クライアントを使用して、ASA との間でファイルをコピーすることができます。ASA は接続先の各 SCP サーバの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバとそのキーを追加または削除できます。

サーバごとに（**server** コマンドを参照）、SSH ホストの **key-string**（公開キー）または **key-hash**（ハッシュ値）を指定できます。

例

次に、10.86.94.170 にあるサーバのすでにハッシュされているホスト キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

次に、10.7.8.9 にあるサーバのホスト ストリング キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

関連コマンド

コマンド	説明
copy	ASA との間でファイルをコピーします。
key-hash	ハッシュ SSH ホスト キーを入力します。
key-string	公開 SSH ホスト キーを入力します。
サーバ	SSH サーバとホスト キーを ASA データベースに追加します。
ssh stricthostkeycheck	オンボードのセキュア コピー(SCP)クライアントの SSH ホスト キーのチェックをイネーブルにします。

ssh scopy enable

ASA で Secure Copy（SCP; セキュア コピー）をイネーブルにするには、グローバル コンフィギュレーション モードで **ssh scopy enable** コマンドを使用します。SCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh scopy enable

no ssh scopy enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(7)/9.4(3)/9.5(3)/9.6(1)	**ssh cipher encryption** コマンドおよび **ssh cipher integrity** コマンドを使用して、SSH アクセスの暗号化と整合性の方式を設定できます。

使用上のガイドライン

SCP はサーバのみの実装です。SCP のための接続を受け入れて終了できますが、開始することはできません。ASA には、次の制約事項があります。

- SCP のこの実装にはディレクトリ サポートはないため、ASA の内部ファイルへのリモート クライアント アクセスは制限されます。
- SCP の使用時はバナー サポートはありません。
- SCP ではワイルドカードはサポートされません。
- SSH バージョン 2 接続をサポートするには、ASA のライセンスに VPN-3DES-AES 機能が必要です。

ファイル転送を開始する前に、ASA では使用可能なフラッシュ メモリをチェックします。使用可能なスペースが十分ではない場合、ASA は SCP 接続を終了します。フラッシュ メモリ内のファイルを上書きする場合でも、ASA にコピーされるファイル用に十分な空きスペースが必要です。SCP プロセスでは、ファイルはまず一時ファイルにコピーされ、置き換えられるファイルに一時ファイルがコピーされます。コピーされるファイルと上書きされるファイルを保持する十分なスペースがフラッシュ内にない場合、ASA は SCP 接続を終了します。

セキュア コピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式を変更するには、たとえば、**ssh cipher encryption custom aes128-cbc** などの **ssh cipher encryption** コマンドを使用します。

例

次の例に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続を受け入れるよう内部インターフェイスを設定する方法を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh scopy enable
ciscoasa(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークから ASA への SSH 接続を許可します。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、ASA を制限します。

ssh stricthostkeycheck

オンボードのセキュア コピー(SCP)クライアントに対する SSH ホスト キー チェックをイネーブルにするには、グローバル コンフィギュレーション モードで **ssh stricthostkeycheck** コマンドを使用します。ホスト キー チェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh stricthostkeycheck

no ssh stricthostkeycheck

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドはデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

オンボードの SCP クライアントを使用して、ASA との間でファイルをコピーすることができます。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

例

次に、SSH ホスト キー チェックをイネーブルにする例を示します。

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?
```

```
Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

関連コマンド

コマンド	説明
copy	ASA との間でファイルをコピーします。
key-hash	ハッシュ SSH ホスト キーを入力します。
key-string	公開 SSH ホスト キーを入力します。
サーバ	SSH サーバとホスト キーを ASA データベースに追加します。
ssh pubkey-chain	ASA のデータベースに格納されるサーバとそのキーを手動で追加または削除します。

ssh timeout

デフォルトの SSH セッション アイドル タイムアウト値を変更するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

ssh timeout *number*

no ssh timeout

構文の説明

number	SSH セッションが切断される前に非アクティブである時間を分単位で指定します。有効な値は、1 ～ 60 分です。

デフォルト

デフォルトのセッション タイムアウト値は、5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ssh timeout コマンドでは、セッションが切断される前にアイドルである時間を分単位で指定します。デフォルトの時間は、5 分です。

例

次に、IP アドレス 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続のみを受け入れるように、内部インターフェイスを設定する例を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
show ssh sessions	ASA とのアクティブ SSH セッションに関する情報を表示します。
ssh disconnect	アクティブな SSH セッションを切断します。

ssh version

ASA が受け入れる SSH のバージョンを制限するには、グローバル コンフィギュレーション モードで **ssh version** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。バージョン 2 のみがサポートされます。

ssh version 2

no ssh version 2

構文の説明

2	SSH バージョン 2 接続のみがサポートされることを指定します。

デフォルト

デフォルトでは、バージョン 2 のみがサポートされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.12(1)	Version **1** キーワードが削除されました。

使用上のガイドライン

バージョン 2 のみがサポートされます。

例

次の例に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続を受け入れるよう内部インターフェイスを設定する方法を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークから ASA への SSH 接続を許可します。

ssl certificate-authentication

8.2(1) よりも前のバージョンに対する下位互換性のためにクライアント証明書の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ssl certificate-authentication** コマンドを使用します。ssl 証明書の認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ssl certificate-authentication interface *interface-name* **port** *port-number*

no ssl certificate-authentication interface *interface-name* **port** *port-numbe***r**

構文の説明

interface-name	選択したインターフェイスの名前。inside、management、outside などです。
port-number	TCP ポート番号。1 ～ 65535 の範囲の整数です。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドが追加されました。
8.2(1)	このコマンドは不要になりましたが、以前のバージョンにダウングレードする場合に備えて、ASA で保持されています。

使用上のガイドライン

このコマンドは、廃止された **http authentication-certificate** コマンドに代わるものです。

例

次に、SSL 証明書認証機能を使用するように ASA を設定する例を示します。

```
ciscoasa(config)# ssl certificate-authentication interface inside port 330
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。

ssl cipher

SSL、DTLS、TLS の各プロトコル用の暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **ssl cipher** コマンドを使用します。デフォルト（暗号化アルゴリズムの完全なセット）に戻すには、このコマンドの **no** 形式を使用します。

ssl cipher *version* [*level* | **custom** "*string*"]

no ssl cipher *version* [*level* | **custom** "***string***"]

構文の説明

custom *string*	OpenSSL 暗号定義文字列を使用して暗号スイートの完全な制御権限を付与します。
level	暗号強度を指定し、サポートされる暗号の最低レベルを示します。次に、強度の有効な値を強度の低い順に示します。 • **all**：NULL-SHA を含むすべての暗号が含まれます。 • **low**：NULL-SHA を除くすべての暗号が含まれます。 • **medium**：NULL-SHA、DES-CBC-SHA、および RC4-MD5 を除くすべての暗号が含まれます。 • **fips**：FIPS 準拠の暗号がすべて含まれます（NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く）。 • **high**（TLSv1.2 にのみ適用）：SHA-2 暗号を使用する AES-256 のみが含まれます。
version	SSL、DTLS、TLS プロトコルのバージョンを指定します。サポートされているバージョンは次のとおりです。 • **default**：発信接続用の暗号セット。 • **dtlsv1**：DTLSv1 着信接続用の暗号。 • **dtlsv1.2**：DTLSv1.2 着信接続用の暗号。 • **tlsv1**：TLSv1 着信接続用の暗号。 • **tlsv1.1**：TLSv1.1 着信接続用の暗号。 • **tlsv1.2**：TLSv1.2 着信接続用の暗号。

デフォルト

すべてのプロトコル バージョンのデフォルトは、**medium** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。
9.4(1)	すべての SSLv3 設定とサポートが ASA から削除されました。
9.10(1)	dtls 1.2 オプションが追加されました。
9.12(1)	lina で tlv1 でサポートされている暗号から NULL-SHA を削除しました。ssl cipher tlsv1 all および ssl cipher tlsv1 custom NULL-SHA コマンドが廃止され削除されました。

使用上のガイドライン

このコマンドは、ASA Version 9.3(2) から **ssl encryption** コマンドに置き換わりました。

推奨設定は **medium** です。**high** を使用すると、接続が制限される場合があります。**custom** を使用すると、少数の暗号のみが設定されている場合は、機能が制限されることがあります。デフォルトのカスタム値を制限すると、クラスタリングを含めて発信接続が制限されることがあります。

OpenSSL を使用した暗号の詳細については、https://www.openssl.org/docs/apps/ciphers.html を参照してください。

どの暗号がどのバージョンをサポートしているかのリストを表示するには、**show ssl ciphers all** コマンドを使用します。次に例を示します。

```
These are the ciphers for the given cipher level; not all ciphers are supported by all
versions of SSL/TLS.
These names can be used to create a custom cipher list:
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DES-CBC3-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  RC4-SHA (sslv3, tlsv1)
  RC4-MD5 (sslv3, tlsv1)
  DES-CBC-SHA (sslv3, tlsv1)
  NULL-SHA (sslv3, tlsv1)
```

ASA では、サポートされる暗号の優先順位が次のように指定されています。

TLSv1.2 でサポートされている暗号（1 ～ 9）

1. DHE-RSA-AES256-SHA256
2. AES256-SHA256
3. DHE-RSA-AES128-SHA256
4. AES128-SHA256
5. DHE-RSA-AES256-SHA
6. AES256-SHA
7. DHE-RSA-AES128-SHA
8. AES128-SHA
9. DES-CBC3-SHA

TLSv1.1 または TLSv1.2 でサポートされていない暗号（10 ～ 13）

10. RC4-SHA
11. RC4-MD5
12. DES-CBC-SHA
13. NULL-SHA

例

次に、TLSv1.1 FIPS 準拠の暗号を使用するように ASA を設定する例を示します。

```
ciscoasa(config)# ssl cipher tlsv1.1 fips
```

次に、TLSv1 カスタム暗号を使用するように ASA を設定する例を示します。

```
ciscoasa(config)# ssl cipher tlsv1 custom "RC4-SHA:ALL"
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
show ssl ciphers	サポートされている暗号のリストを表示します。

ssl client-version

ASA がクライアントとして動作する場合の SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl client-version** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

ssl client-version [**any** | **sslv3-only** | **tlsv1-only** | **sslv3** | **tlsv1** | **tlsv1.1** | **tlsv1.2**]

no ssl client-version

構文の説明

任意	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
sslv3	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
sslv3-only	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。 **（注）** このオプションは、バージョン 9.3(2) で廃止されました。
tlsv1	TLSv1 クライアントの hello を送信し、TLSv1（以降）をネゴシエートします。
tlsv1.1	TLSv1.1 クライアントの hello を送信し、TLSv1.1（以降）をネゴシエートします。
tlsv1.2	TLSv1.2 クライアントの hello を送信し、TLSv1.2（以降）をネゴシエートします。
tlsv1-only	TLSv1 クライアントの hello を送信し、TLSv1（以降）をネゴシエートします。 **（注）** このオプションは、バージョン 9.3(2) で廃止されました。

デフォルト

デフォルト値は、**tlsv1** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(2)	SSLv3 は廃止されました。現在のデフォルトは [any] ではなく [tlsv1] です。[any] キーワードは廃止されました。

使用上のガイドライン

any、**sslv3**、または **sslv3-only** キーワードを使用した場合、次の警告が表示されますが、コマンドは受け入れられます。

```
WARNING: SSLv3 is deprecated. Use of TLSv1 or greater is recommended.
```

ASA の次のメジャー リリースでは、これらのキーワードは ASA から削除されます。

例

次に、SSL クライアントとして動作する場合に SSLv3 プロトコルのバージョンを指定するように ASA を設定する例を示します。

```
ciscoasa(config)# ssl client-version any
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl server-version	ASA が SSL/TLS 接続をネゴシエートする最小プロトコル バージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl dh-group

TLS が使用する DHE-RSA 暗号で Diffie-Hellmann（DH）グループを使用するように指定するには、グローバル コンフィギュレーション モードで **ssl dh-group** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]

no ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]

構文の説明

group1	DH グループ 1（768 ビット モジュラス）を設定します。
group2	DH グループ 2（1024 ビット モジュラス）を設定します。
group5	DH グループ 5（1536 ビット モジュラス）を設定します。
group14	DH グループ 14（2048 ビット モジュラス、224 ビット素数位数サブグループ）を設定します。
group24	DH グループ 24（2048 ビット モジュラス、256 ビット素数位数サブグループ）を設定します。

デフォルト

デフォルトは DH グループ 14 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。
9.13(1)	**group2** および **group 5** コマンド オプションは廃止され、以降のリリースで削除されます。

使用上のガイドライン

グループ 1 および 2 は、Java 7 およびそれ以前のバージョンと互換性があります。グループ 5、14、および 24 は、Java 7 と互換性がありません。すべてのグループが Java 8 と互換性があります。グループ 14 と 24 は FIPS 準拠です。

例

次に、特定の DH グループを使用するように ASA を設定する例を示します。

```
ciscoasa(config)# ssl dh-group group14
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。

ssl ecdh-group

TLS が使用する ECDHE-ECDSA 暗号でグループを使用するように指定するには、グローバル コンフィギュレーション モードで **ssl ecdh-group** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

ssl ecdh-group [**group19** | **group20** | **group21**]

no ssl ecdh-group [**group19** | **group20** | **group21**]

構文の説明

group19	グループ 19（256 ビット EC）を設定します。
group20	グループ 20（384 ビット EC）を設定します。
group21	グループ 21（521 ビット EC）を設定します。

デフォルト

デフォルトはグループ 19 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

TLSv1.2 では、次の暗号方式のサポートが追加されています。

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256

- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

(注) 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。

例

次に、特定の DH グループを使用するように ASA を設定する例を示します。

```
ciscoasa(config)# ssl ecdh-group group21
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。

ssl encryption（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.3(1) でした。

SSL、DTLS、TLS の各プロトコル用の暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **ssl encryption** コマンドを使用します。デフォルト（暗号化アルゴリズムの完全なセット）に戻すには、このコマンドの **no** 形式を使用します。

ssl encryption [**3des-sha1**] [**aes128-sha1**] [**aes256-sha1**] [**des-sha1**] [**null-sha1**] [**rc4-md5**] [**rc4-sha1**] [**dhe-aes256-sha1**] [**dhe-aes128-sha1**]

no ssl encryption

構文の説明

3des-sha1	Secure Hash Algorithm 1 を使用する Triple DES 168 ビット暗号化を指定します（FIPS 準拠）。
aes128-sha1	Secure Hash Algorithm 1 を使用するトリプル AES 128 ビット暗号化を指定します（FIPS 準拠）。
aes256-sha1	Secure Hash Algorithm 1 を使用するトリプル AES 256 ビット暗号化を指定します（FIPS 準拠）。
dhe-aes128-sha1	Transport Layer Security（TLS）用に AES 128 ビット暗号化暗号スイートを指定します（FIPS 準拠）。
dhe-aes256-sha1	Transport Layer Security（TLS）用に AES 256 ビット暗号化暗号スイートを指定します（FIPS 準拠）。
des-sha1	Secure Hash Algorithm 1 を使用する DES 56 ビット暗号化を指定します。
null-sha1	Secure Hash Algorithm 1 で使用するヌル暗号化を指定します。この設定は、機密性なしでメッセージ整合性を強化します。 **注意** **null-sha1** を指定すると、データは暗号化されません。
rc4-md5	MD5 ハッシュ関数を使用する RC4 128 ビット暗号化を指定します。
rc4-sha1	Secure Hash Algorithm 1 を使用する RC4 128 ビット暗号化を指定します。

デフォルト

デフォルトでは、ASA 上の SSL 暗号化リストには次のアルゴリズムが次の順序で含まれています。

1. RC4-SHA1
2. AES128-SHA1（FIPS 準拠）
3. AES256-SHA1（FIPS 準拠）
4. 3DES-SHA1（FIPS 準拠）
5. DHE-AES256-SHA1（FIPS 準拠）
6. DHE-AES128-SHA1（FIPS 準拠）

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(2)	DHE-AES128-SHA1 アルゴリズムおよび DHE-AES256-SHA1 アルゴリズムを使用した SSL 暗号化のサポートが追加されました。
9.3(2)	このコマンドは廃止され、**ssl cipher** コマンドに置き換えられました。
9.12(1)	このコマンドは削除されました。

使用上のガイドライン

このコマンドを再度発行すると、前の設定は上書きされます。ASDM のライセンス タブには、設定した値ではなく、ライセンスでサポートされる暗号化の最大レベルが反映されます。

アルゴリズムの使用の優先順位は、アルゴリズムの順序によって決まります。環境のニーズに合わせてアルゴリズムを追加または削除できます。

FIPS 準拠の AnyConnect クライアント SSL 接続の場合、FIPS 準拠の暗号が SSL 暗号化リストの先頭に指定されていることを確認する必要があります。

アプリケーションによっては DHE がサポートされないものがあるため、他の SSL 暗号化方式を少なくとも 1 つ含めて、暗号スイートが両方に共通するようにします。

http://en.wikipedia.org/wiki/Symmetric-key_algorithm に示すように、暗号化操作では対称キー アルゴリズムが使用されます。

例

次に、3des-sha1 および des-sha1 暗号化アルゴリズムを使用するように ASA を設定する例を示します。

```
ciscoasa(config)# ssl encryption 3des-sha1 des-sha1
```

ASA Version 9.3(2) 以降

次の例では、このコマンドが廃止され、**ssl cipher** コマンドに置き換えられたことを示します。

```
ciscoasa(config)# ssl encryption ?

configure mode commands/options:
This command is DEPRECATED, use 'ssl cipher' instead.

  3des-sha1         Indicate use of 3des-sha1 for ssl encryption
  aes128-sha1       Indicate use of aes128-sha1 for ssl encryption
  aes256-sha1       Indicate use of aes256-sha1 for ssl encryption
  des-sha1          Indicate use of des-sha1 for ssl encryption
  dhe-aes128-sha1   Indicate use of dhe-aes128-sha1 for ssl encryption
```

```
  dhe-aes256-sha1  Indicate use of dhe-aes256-sha1 for ssl encryption
  null-sha1        Indicate use of null-sha1 for ssl encryption (NOTE: Data is
                   NOT encrypted if this cipher is chosen)
  rc4-md5          Indicate use of rc4-md5 for ssl encryption
  rc4-sha1         Indicate use of rc4-sha1 for ssl encryption

ciscoasa(config)# ssl encryption rc4-sha1 aes256-sha1 aes128-sha1

WARNING: This command has been deprecated; use 'ssl cipher' instead.
INFO: Converting to: ssl cipher default custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher sslv3 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher tlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher dtlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	ASA が SSL/TLS 接続をネゴシエートする最小プロトコル バージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。
ssl cipher	SSL、DTLS、および TLS プロトコルの暗号化アルゴリズムを指定します。 (注)　9.3(2) リリース以降で使用できます。

ssl server-version

ASA が SSL/TLS 接続をネゴシエートする最小プロトコル バージョンを設定するには、グローバル コンフィギュレーション モードで **ssl server-version** コマンドを使用します。デフォルトの any に戻すには、このコマンドの **no** 形式を使用します。

ssl server-version [[**tlsv1** | **tlsv1.1** | **tlsv1.2**] [**dtlsv1** | **dtlsv1.2**]]

no ssl server-version

構文の説明

tlsv1	SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートします。
tlsv1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートします。
tlsv1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートします。
dtlsv1	DTLSv1 クライアントの hello を受け入れ、DTLSv1（以降）をネゴシエートします。
dtlsvv 1.2	DTLSv1.2 クライアントの hello を受け入れ、DTLSv1.2（以降）をネゴシエートします。DTLSv 1.2 トンネルの使用を指定するには、唯一の有効なオプションである TLSv 1.2 トンネルの指定が必要です。

デフォルト

デフォルト値は **tlsv1** および **dtlsv1** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(2)	SSLv3 は廃止されました。現在のデフォルトは [any] ではなく [tlsv1] です。[any] キーワードは廃止されました。

リリース	変更内容
9.4(1)	すべての SSLv3 キーワードが ASA コンフィギュレーションから削除され、SSLv3 サポートが ASA から除外されました。SSLv3 がイネーブルになっている場合は、SSLv3 オプションを指定したコマンドからブート時エラーが表示されます。ASA はデフォルトの TLSv1 に戻ります。
9.10(1)	DTLSv 1.2 がサポートされるようになり、DTLS オプションが提供されるようになりました。以前は、DTLS バージョン 1 がデフォルトのままと想定されていました。

使用上のガイドライン

例

次に、SSL/TLS 接続をネゴシエートするように ASA を設定する例を示します。

```
ciscoasa(config)# ssl server-version tlsv1
```

次に、set versions のコンフィギュレーションおよび検証の例を示します。

```
ciscoasa (config)# ssl server-version tlsv1.2 dtlsv1.2
ciscoasa (config)# sh run ssl
ssl server-version tlsv1.2 dtlsv1.2

ciscoasa (config)# no ssl server-version
ciscoasa (config)# sh run all ssl
ssl server-version tlsv1 dtlsv1
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl trust-point

インターフェイスの SSL 証明書を表す証明書トラストポイントを指定するには、グローバル コンフィギュレーション モードで **ssl trust-point** コマンドを *interface* 引数を指定して使用します。インターフェイスを指定しない SSL トラストポイントをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。インターフェイスを指定するエントリを削除するには、このコマンドの **no ssl trust-point** *name* [*interface*] 形式を使用します。

ssl trust-point *name* [*interface* [**vpnlb-ip**] | **domain** *domain-name*]

no ssl trust-point *name* [*interface* [**vpnlb-ip**] | **domain** ***domain-name***]

構文の説明

domain *domain-name*	このインターフェイスへのアクセスに使用される特定のドメイン名（たとえば、www.cisco.com）にこのトラストポイントを関連付けます。
interface	トラストポイントが適用されるインターフェイスの名前を指定します。インターフェイスの名前は **nameif** コマンドで定義します。
name	**crypto ca trustpoint** *name* コマンドに設定されているように CA トラストポイントの名前を指定します。
vpnlb-ip	このインタ ーフェイスの VPN ロード バランシング クラスタ IP アドレスにこのトラストポイントを関連付けます。インターフェイスにだけ適用されます。

デフォルト

デフォルトでは、トラストポイント アソシエーションはありません。ASA では、デフォルトの自己生成 RSA キー ペア証明書が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(2)	**domain** *domain-name* のキーワードと引数の組み合わせが追加されました。

使用上のガイドライン

インターフェイスまたはドメインを指定しない場合、このエントリは、独自のトラストポイントに関連付けられていない、すべてのインターフェイスで使用されるフォールバック トラストポイントを表します。

ssl trustpoint ? コマンドを入力すると、使用可能な設定済みのトラストポイントが表示されます。**ssl trust-point** *name* **?** コマンド（たとえば、**ssl trust-point mysslcert ?**）を入力した場合、trustpoint-SSL 証明書アソシエーションに使用可能な設定済みのインターフェイスが表示されます。

インターフェイス 1 つにつき、最大 16 個のトラストポイントを設定できます。

このコマンドを使用するときは、次のガイドラインに従ってください。

- *trustpoint* の値は、**crypto ca trustpoint** *name* コマンドで設定された CA トラストポイントの name である必要があります。
- *interface* の値は、あらかじめ設定されたインターフェイスの *nameif* 名である必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照する **ssl trust-point** エントリも削除されます。
- **ssl trust-point** エントリは、インターフェイスごとに 1 つと、インターフェイスを指定しないもの 1 つを保持できます。
- **domain** キーワードで設定したトラストポイントは、複数のインターフェイスに適用されることがあります（接続方法によって異なります）。
- *domain-name* 値ごとに **ssl trust-point** を 1 つだけ設定できます。
- 同じトラストポイントを複数のエントリで再利用できます。
- このコマンドを入力すると、次のエラーが表示される場合があります。

  ```
  error:0B080074:x509 certificate routines:X509_check_private_key:key values
  mismatch@x509_cmp.c:339
  ```

  これは、ユーザが新しい証明書を設定して、以前に設定された証明書と置き換えたことを示しています。特に対処の必要はありません。
- 証明書は次の順序で選択されます。
  - 接続が **domain** キーワードの値に一致した場合、その証明書が最初に選択されます。（**ssl trust-point** *name* **domain** *domain-name* コマンド）
  - ロード バランシング アドレスへの接続が確立された場合、vpnlb-ip 証明書が選択されます。（**ssl trust-point** *name* **interface vpnlb-ip** コマンド）
  - インターフェイスに対して設定された証明書。（**ssl trust-point** *name* **interface** コマンド）
  - インターフェイスに関連付けられていないデフォルトの証明書。（**ssl trust-point** *name* コマンド）
  - ASA の自己署名付き自己生成証明書。

例

次に、inside インターフェイスの FirstTrust という名前の SSL トラストポイントと、インターフェイスが関連付けられない DefaultTrust という名前のトラストポイントを設定する例を示します。

```
ciscoasa(config)# ssl trust-point FirstTrust inside
ciscoasa(config)# ssl trust-point DefaultTrust
```

次に、このコマンドの **no** 形式を使用して、インターフェイスが関連付けられていないトラストポイントを削除する例を示します。

```
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa(config)# no ssl trust-point
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

次に、インターフェイスが関連付けられているトラストポイントを削除する例を示します。

```
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa(config)# no ssl trust-point FirstTrust inside
ciscoasa(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

次に、設定済みのトラストポイントに特定のドメイン名を割り当てる例を示します。

```
ciscoasa(config)# ssl trust-point www-cert domain www.example.com
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl server-version	ASA が SSL/TLS 接続をネゴシエートする最小プロトコル バージョンを指定します。
show ssl	SSL 設定統計情報を表示します。

sso-server（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

ASA のユーザ認証のために Single Sign-On（SSO; シングル サインオン）サーバを作成する場合、webvpn コンフィギュレーション モードで **sso-server** コマンドを使用します。このコマンドでは、SSO サーバ タイプを指定する必要があります。

SSO サーバを削除するには、このコマンドの **no** 形式を使用します。

sso-server *name* **type** [*siteminder* | *saml-v1.1-post*]

no sso-server *name*

(注) このコマンドは、SSO 認証用に必要です。

構文の説明

name	SSO サーバの名前を指定します。最小 4 文字、最大 31 文字です。
saml-v1.1-post	設定する ASA SSO サーバが、SAML、バージョン 1.1、POST タイプの SSO サーバであることを指定します。
siteminder	設定する ASA SSO サーバが、Computer Associates SiteMinder SSO サーバであることを指定します。
type	SSO サーバのタイプを指定します。使用できるタイプは、SiteMinder と SAML-V1.1-POST だけです。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**sso-server** コマンドを使用すると、SSO サーバを作成できます。

認証では、ASA は SSO サーバへの WebVPN ユーザのプロキシとして動作します。ASA は現在、SiteMinder SSO サーバ（以前の Netegrity SiteMinder）と SAML POST タイプの SSO サーバをサポートしています。現在、type オプションで使用できる引数は *siteminder* または *saml-V1.1-post* に限定されています。

例

次に、webvpn コンフィギュレーション モードで、「example1」という名前の SiteMinder-type の SSO サーバを作成する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example1 type siteminder
ciscoasa(config-webvpn-sso-siteminder)#
```

次に、webvpn コンフィギュレーション モードで、「example2」という名前の SAML、バージョン 1.1、POST-type の SSO サーバを作成する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example2 type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml)#
```

関連コマンド

コマンド	説明
assertion-consumer-url	SAML-type の SSO アサーション コンシューマ サービスの URL を指定します。
issuer	SAML-type の SSO サーバのセキュリティ デバイス名を指定します。
max-retry-attempts	ASA が、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの運用統計情報を表示します。
test sso-server	テスト認証要求で SSO サーバをテストします。
トラストポイント	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

sso-server value（group-policy webvpn）（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

SSO サーバをグループ ポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで使用可能な webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。

割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。

デフォルト ポリシーが継承されないようにするには、**sso-server none** コマンドを使用します。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

構文の説明

name	グループ ポリシーに割り当てる SSO サーバの名前を指定します。

デフォルト

グループに割り当てられるデフォルト ポリシーは、DfltGrpPolicy です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

グループ ポリシー webvpn モードで **sso-server value** コマンドを入力すると、SSO サーバをグループ ポリシーに割り当てることができます。

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。ASA は、現在、SiteMinder-type の SSO サーバと SAML POST-type の SSO サーバをサポートしています。

このコマンドは SSO サーバの両タイプに適用されます。

(注) SSO サーバをユーザ ポリシーに割り当てるには、同じコマンド **sso-server value** をユーザ名 webvpn コンフィギュレーション モードで入力します。

例

次に、グループ ポリシー my-sso-grp-pol を作成し、example という名前の SSO サーバに割り当てるサンプル コマンドを示します。

```
ciscoasa(config)# group-policy my-sso-grp-pol internal
ciscoasa(config)# group-policy my-sso-grp-pol attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# sso-server value example
ciscoasa(config-group-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
sso-server value（ユーザ名 **webvpn**）	SSO サーバをユーザ ポリシーに割り当てます。
web-agent-url	ASA が、SiteMinder-type の SSO 認証を要求する SSO サーバの URL を指定します。

sso-server value（username webvpn）（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

SSO サーバをユーザ ポリシーに割り当てるには、ユーザ名コンフィギュレーション モードで使用可能な webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。

ユーザの SSO サーバ割り当てを削除するには、このコマンドの **no** 形式を使用します。

ユーザ ポリシーがグループ ポリシーから不要な SSO サーバ割り当てを継承している場合は、**sso-server none** コマンドを使用して割り当てを削除します。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

構文の説明

name	ユーザ ポリシーに割り当てる SSO サーバの名前を指定します。

デフォルト

デフォルトでは、ユーザ ポリシーはグループ ポリシーの SSO サーバ割り当てを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。ASA は、現在、SiteMinder-type の SSO サーバと SAML POST-type の SSO サーバをサポートしています。

このコマンドは SSO サーバの両タイプに適用されます。

sso-server value コマンドを入力すると、SSO サーバをユーザ ポリシーに割り当てることができます。

(注) SSO サーバをグループ ポリシーに割り当てるには、同じコマンド **sso-server value** をグループ webvpn コンフィギュレーション モードで入力します。

例

次に、my-sso-server という名前の SSO サーバを Anyuser という名前の WebVPN ユーザのユーザ ポリシーに割り当てるサンプル コマンドを示します。

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# sso-server value my-sso-server
ciscoasa(config-username-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
sso-server value（**config-group-webvpn**）	SSO サーバをグループ ポリシーに割り当てます。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

start-port

マッピングアドレスおよびポート(MAP)ドメイン内の基本マッピングルールでポートプールの開始ポートを設定するには、MAP ドメインの基本マッピング ルール コンフィギュレーション モードで **start-port** コマンドを使用します。比率を削除するには、このコマンドの **no** 形式を使用します。

start-port *number*

no start-port *number*

構文の説明

number	変換されたアドレスのポートプールに表示される最初のポート。指定するポートは 1 ～ 32768 の範囲内とし、2 の累乗にする必要があります(1、2、4、8 など)。既知のポートを除外する場合は、1024 以降から開始します。

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
MAP ドメインの基本マッピング ルール コンフィギュレーション モード。	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが導入されました。

使用上のガイドライン

基本マッピングルールの **start-port** コマンドおよび **share-ratio** コマンドによって、MAP ドメイン内のアドレス変換に使用されるプールの開始ポートとポート数が決まります。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
```

```
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート(MAP)ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート(MAP)ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

start-url

オプションの事前ログイン クッキーの取得先 URL を入力するには、AAA サーバ ホスト コンフィギュレーション モードで **start-url** コマンドを入力します。これは HTTP フォームのコマンドを使用した SSO です。

start-url *string*

(注) HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	SSO サーバの URL。URL の最大長は 1024 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA の WebVPN サーバは、HTTP POST 要求を使用して、シングル サインオン認証要求を認証 Web サーバに送信できます。認証 Web サーバは、Set-Cookie ヘッダーをログイン ページのコンテンツとともに送信することによって、事前ログイン シーケンスを実行できます。このことは、認証 Web サーバのログイン ページにブラウザで直接接続することによって検出できます。ログイン ページがロードされるときに Web サーバによってクッキーが設定され、このクッキーがその後のログイン セッションに関連する場合、**start-url** コマンドを使用してクッキーの取得先 URL を入力する必要があります。実際のログイン シーケンスは、事前ログイン クッキー シーケンスの後で、認証 Web サーバへのフォーム送信により開始されます。

(注) **start-url** コマンドは、事前ログイン クッキー交換が存在する場合にのみ必要です。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、事前ログイン クッキーを取得するための URL https://example.com/east/Area.do?Page-Grp1 を指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 (inside) host example.com
ciscoasa(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

state-checking

H.323 の状態チェックを実行するには、パラメータ コンフィギュレーション モードで **state-checking** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

state-checking [h225 | ras]

no state-checking [h225 | ras]

構文の説明

h225	H.225 の状態チェックを実行します。
ras	RAS の状態チェックを実行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 コールで RAS の状態チェックを実行する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# state-checking ras
```

関連コマンド

コマンド	説明
policy-map type inspect	インスペクション ポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

storage-url

各コンテキストでフラッシュ メモリを使用して VPN パッケージを格納できるようにするには、コンテキスト コンフィギュレーション モードで **storage-url** コマンドを使用します。記憶域を削除するには、このコマンドの **no** 形式を使用します。

storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

no storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

構文の説明

private	プライベート記憶域をコンテキストに割り当てます。private で指定できる専用記憶域は、コンテキストごとに 1 つに限られます。
共有	共有記憶域をコンテキストに割り当てます。shared で指定できる読み取り専用の共有記憶域はコンテキストごとに 1 つですが、共有ディレクトリは複数作成することができます。
[**disk***n***:/**]*path*	記憶域にパスを設定します。ディスク番号を指定しない場合、デフォルトで **disk0** に設定されます。ASA はプライベート記憶域に指定されたパスの下にサブディレクトリを作成し、コンテキストにちなんだ名前を付けます。たとえば、contextA の場合、**disk1:/private-storage** をパスとして指定すると、ASA はこのコンテキストのサブディレクトリを disk1:/private-storage/contextA/ に作成します。この記憶域は複数のコンテキストで共有されるため、ASA は共有記憶域にはコンテキストのサブディレクトリを作成しません。
context_label	(オプション)ファイル システムがコンテキスト管理者に公開されないよう、このパスにコンテキスト内での名前を指定することもできます。それには、*context_label* を使用します。たとえば、*context_label* を **context** として指定すると、コンテキスト内からは、このディレクトリは **context:** と呼ばれます。

コマンド デフォルト

ディスク番号を指定しない場合、デフォルトで **disk0** に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

各コンテキストで、フラッシュ メモリを使用して AnyConnect などの VPN パッケージを保存できるだけでなく、AnyConnect およびクライアントレス SSL VPN ポータルのカスタマイズのストレージも提供できるようにします。読み取り専用の共有記憶域だけでなく、コンテキストごとに専用の記憶域も使用できます。注:**mkdir** コマンドを使用して、指定するディスク上にターゲット ディレクトリがすでに存在することを確認してください。

private で指定できる専用記憶域は、コンテキストごとに 1 つに限られます。コンテキスト内から（およびシステム実行スペースから）、このディレクトリの読み取り/書き込み/削除操作を実行できます。コンテキストごとに許容するディスク容量の大きさを制御するには、**limit-resource storage** コマンドを参照してください。

AnyConnect パッケージなど、すべてのコンテキストに共通の大きなファイルを共有記憶域で共有することで、ASA は大きなファイルの重複を抑えることができます。共有ディレクトリの書き込みおよび削除操作は、システム実行スペースでのみ実行できます。

例

次に、プライベート ディレクトリと共有ディレクトリを作成し、それらを管理コンテキストに割り当てる例を示します。

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

関連コマンド

コマンド	説明
limit-resource storage	コンテキストごとに許容するディスク容量の大きさを制御します。

storage-key

セッション間に保管されるデータを保護するストレージ キーを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **storage-key** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

storage- key {**none** | **value** *string*}

no storage-key

構文の説明

string	ストレージ キーの値として使用するストリングを指定します。この文字列は最大 64 文字まで使用できます。

デフォルト

デフォルトは **none** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ストレージ キーの値にはスペース以外の任意の文字を使用できますが、標準的な英数字セット(0 ～ 9 および a ～ z)のみを使用することを推奨します。

例

次に、ストレージ キーを値 abc123 に設定する例を示します。

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# storage-key value abc123
```

関連コマンド

コマンド	説明
storage-objects	セッションとセッションの間に保存されたデータのストレージ オブジェクトを設定します。

storage-objects

セッション間に保管されるデータについて使用するストレージ オブジェクトを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **storage-objects** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

storage- objects {**none** | **value** *string*}

no storage-objects

構文の説明

string	ストレージ オブジェクトの名前を指定します。この文字列は最大 64 文字まで使用できます。

デフォルト

デフォルトは **none** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ストレージ オブジェクト名にはスペースおよびカンマ以外の任意の文字を使用できますが、標準的な英数字セット(0 ～ 9 および a ～ z)のみを使用することを推奨します。ストリング内でストレージ オブジェクトの名前を区切るには、カンマをスペースなしで使用します。

例

次に、ストレージ オブジェクト名を cookies および xyz456 に設定する例を示します。

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# storage-object value cookies,xyz456
```

関連コマンド

コマンド	説明
storage-key	セッション間に保管されるデータに対して使用するストレージ キーを設定します。
user-storage	セッション間にユーザ データを保管するための場所を設定します。

strict-asp-state

M3UA アプリケーション サーバ プロセス（ASP）の厳密な状態検証を有効にするには、ポリシー マップ パラメータ コンフィギュレーショ モードで **strict-asp-state** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

strict-asp-state

no strict-asp-state

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、M3UA インスペクション ポリシー マップを設定する場合に使用します。

アプリケーション サーバ プロセス（ASP）の厳密な状態検証を有効にすると、システムは M3UA セッションの ASP の状態を維持し、検証結果に基づいて ASP メッセージを許可またはドロップします。ASP の厳密な状態検証を無効にすると、すべての ASP メッセージが検査されずに転送されます。

厳密な ASP のステート チェックが必要なのは、ステートフル フェールオーバーが必要な場合、またはクラスタ内での動作が必要な場合です。ただし、厳密な ASP のステート チェックは、上書きモードでのみ動作し、ロードシェアリングまたはブロードキャスト モードで実行している場合は動作しません（RFC 4666 より）。インスペクションは、エンドポイントごとに ASP が 1 つだけあると仮定します。

例

次に、状態およびセッションの厳密なチェックを有効にする例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# strict-asp-state
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect m3ua	M3UA インスペクション ポリシー マップを作成します。

strict-diameter

Diameter プロトコルの RFC 6733 への厳密な準拠を有効にするには、ポリシー マップ パラメータ コンフィギュレーション モードで **strict-diameter** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

strict-diameter {**state** | **session**}

no strict-diameter {**state** | **session**}

構文の説明

state	ステート マシンの検証を有効にします。
session	セッション関連のメッセージの検証を有効にします。

デフォルト

デフォルトでは、インスペクションによって、Diameter フレームの RFC への準拠は確保されますが、状態とセッションのチェックは有効になりません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが導入されました。

使用上のガイドライン

Diameter インスペクション ポリシー マップを設定する場合に、このコマンドを使用します。

これらのオプションでは、標準プロトコルの準拠チェックに加え、状態とセッションの厳密なコンプライアンス検証も有効になります。コマンドを 2 回入力すると、状態とセッションの両方のチェックを有効にすることができます。

例

次に、状態およびセッションの厳密なチェックを有効にする例を示します。

```
ciscoasa(config)# policy-map type inspect diameter diameter-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# strict-diameter state
ciscoasa(config-pmap-p)# strict-diameter session
```

関連コマンド

コマンド	説明
inspect diameter	Diameter インスペクションを有効にします。
policy-map type inspect diameter	Diameter インスペクション ポリシー マップを作成します。

strict-header-validation

RFC 3261 に従って、SIP メッセージのヘッダー フィールドの厳密な検証をイネーブルにするには、パラメータ コンフィギュレーション モードで **strict-header-validation** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

strict-header-validation action {drop | drop-connection | reset | log} [log]

no strict-header-validation action {drop | drop-connection | reset | log} [log]

構文の説明

drop	検証発生時にパケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
ログ	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。任意のアクションと関連付けることができます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップで SIP ヘッダー フィールドの厳密な検証をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# strict-header-validation action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

strict-http

HTTP に準拠していないトラフィックの転送を許可するには、HTTP マップ コンフィギュレーション モードで **strict-http** コマンドを使用します。このモードには **http-map** コマンドを使用してアクセスできます。この機能をデフォルトの動作にリセットするには、このコマンドの **no** 形式を使用します。

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

アクション	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
ログ	（任意）syslog を生成します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信して接続を閉じます。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

厳密な HTTP インスペクションをディセーブルにすることはできませんが、**strict-http action allow** コマンドを使用すると、HTTP に準拠していないトラフィックの転送が ASA で許可されます。このコマンドによって、デフォルトの動作（HTTP に準拠していないトラフィックの転送を拒否する）が上書きされます。

例

次に、HTTP に準拠していないトラフィックの転送を許可する例を示します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# strict-http allow
ciscoasa(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

strip-group

このコマンドは、user@realm の形式で受信されるユーザ名にのみ適用されます。レルムは、ユーザ名に「@」デリミタが付加された管理ドメインです（juser@abc）。

グループ除去処理をイネーブルまたはディセーブルにするには、トンネル グループ一般属性モードで **strip-group** コマンドを使用します。ASA では、VPN クライアントによって提示されるユーザ名からグループ名を取得して、IPsec 接続のトンネル グループを選択します。グループ除去処理をイネーブルにすると、ASA では、ユーザ名のユーザ部分のみを認可/認証のために送信します。それ以外の場合（ディセーブルの場合）、ASA ではレルムを含むユーザ名全体を送信します。

グループ除去処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

strip-group

no strip-group

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

この属性は、IPsec リモート アクセス トンネル タイプだけに適用できます。

（注） MSCHAPv2 の制限により、MSCHAPv2 を PPP 認証に使用すると、トンネル グループのスイッチングを実行できません。MSCHAPv2 中のハッシュ計算はユーザ名の文字列にバインドされます（ユーザ + 区切り + グループなど）。

例

次に、IPsec リモート アクセス タイプの「remotegrp」という名前のリモート アクセス トンネル グループを設定し、一般コンフィギュレーション モードを開始し、「remotegrp」という名前のトンネル グループをデフォルトのグループ ポリシーとして設定して、そのトンネル グループに対してグループ除去をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-group
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

strip-realm

レルム除去処理をイネーブルまたはディセーブルにするには、トンネル グループ一般属性コンフィギュレーション モードで **strip-realm** コマンドを使用します。レルム除去処理によって、ユーザ名を認証サーバまたは認可サーバに送信するときに、ユーザ名からレルムが削除されます。レルムは、@ デリミタを使用してユーザ名に追加される管理ドメインです（username@realm など）。このコマンドをイネーブルにすると、ASA では、ユーザ名のユーザ部分のみを認可/認証のために送信します。それ以外の場合、ASA ではユーザ名全体を送信します。

レルム除去処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

strip-realm

no strip-realm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが追加されました。

使用上のガイドライン

この属性は、IPsec リモート アクセス トンネル タイプだけに適用できます。

例

次に、IPsec リモート アクセス タイプの「remotegrp」という名前のリモート アクセス トンネル グループを設定し、一般コンフィギュレーション モードを開始し、「remotegrp」という名前のトンネル グループをデフォルトのグループ ポリシーとして設定して、そのトンネル グループに対してレルム除去をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-real
```

subject-name コマンド～ sysopt traffic detailed-statistics コマンド

subject-name（暗号 CA 証明書マップ）

IPsec ピア証明書のサブジェクト DN にルール エントリが適用されることを指定するには、クリプト CA 証明書マップ コンフィギュレーション モードで **subject-name** コマンドを使用します。サブジェクト名を削除するには、このコマンドの **no** 形式を使用します。

subject-name [**attr** *tag* **eq | ne |co | nc** *string*]

no subject-name [**attr** *tag* **eq | ne |co | nc** *string*]

構文の説明

attr *tag*	証明書 DN の指定された属性値のみがルール エントリ ストリングと比較されることを指定します。タグ値は次のとおりです。 DNQ = DN 修飾子 GENQ = 世代識別子 I = イニシャル GN = 姓名の名 N = 名前 SN = 姓名の姓 IP = IP アドレス SER = シリアル番号 UNAME = 非構造化名 EA = 電子メール アドレス T = タイトル O = 組織名 L = 地名 SP = 州/都道府県 C = 国 OU = 組織ユニット CN = 一般名
co	ルール エントリ ストリングが DN ストリングまたは指定された属性のサブストリングである必要があることを指定します。
eq	DN ストリングまたは指定された属性がルール ストリング全体と一致する必要があることを指定します。

nc	ルール エントリ ストリングが DN ストリングまたは指定された属性のサブストリングでないことが必要であることを指定します。
ne	DN ストリングまたは指定された属性がルール ストリング全体と一致しないことが必要であることを指定します。
string	照合される値を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA 証明書マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、証明書マップ 1 に対して CA 証明書マップ コンフィギュレーション モードを開始して、証明書サブジェクト名の組織属性が Central と等しくなる必要があることを指定するルール エントリを作成する例を示します。

```
ciscoasa(config)# crypto ca certificate map 1
ciscoasa(ca-certificate-map)# subject-name attr o eq central
ciscoasa(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ コンフィギュレーション モードを開始します。
issuer-name	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

subject-name（暗号 CA トラストポイント）

指定したサブジェクト DN を登録時に証明書に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **subject-name** コマンドを使用します。これは、証明書を使用する人またはシステムです。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

subject-name *X.500_name*

no subject-name

構文の説明

X.500_name	X.500 認定者名を定義します。属性と値のペアを区切るには、カンマを使用します。カンマやスペースを含む値は、引用符で囲みます。たとえば、**cn=crl,ou=certs,o="cisco systems, inc.",c=US** です。最大長は 500 文字です。

デフォルト

デフォルト設定では、サブジェクト名は含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、URL https//:frog.example.com での自動登録を設定し、サブジェクト DN OU certs をトラストポイント central の登録要求に含める例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url http://frog.example.com/
ciscoasa(ca-trustpoint)# subject-name ou=certs
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment url	CA に対する登録用の URL を指定します。

subject-name-default

ローカル CA サーバが発行するすべてのユーザ証明書でユーザ名に追加される一般的なサブジェクト名認定者名(DN)を指定するには、CA サーバ コンフィギュレーション モードで **subject-name-default** コマンドを使用します。サブジェクト名 DN をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

subject-name-default *dn*

no subject-name-default

構文の説明

dn	ローカル CA サーバが発行するすべてのユーザ証明書でユーザ名に含める一般的なサブジェクト名 DN を指定します。サポートされている DN 属性は、cn(一般名)、ou(組織ユニット)、ol(組織の地名)、st(州)、ea(電子メール アドレス)、c(会社)、t(タイトル)、および sn(姓名の姓)です。属性と値のペアを区切るには、カンマを使用します。カンマを含む値は、引用符で囲んでください。*dn* に使用できる文字数は最大 500 文字です。

デフォルト

このコマンドは、デフォルトのコンフィギュレーションの一部ではありません。このコマンドでは、証明書のデフォルトの DN を指定します。ユーザ入力に DN がある場合、このコマンドは ASA によって無視されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

subject-name-default コマンドでは、発行される証明書のサブジェクト名を構成するユーザ名で使用される、共通の一般的な DN を指定します。この目的には、*dn* 値は cn=username で十分です。このコマンドによって、ユーザごとに個別にサブジェクト名 DN を定義する必要がなくなります。**crypto ca server user-db add** dn *dn* コマンドを使用してユーザが追加される場合、DN フィールドは任意です。

ASA では、このコマンドは、ユーザ入力で DN が指定されない場合に、証明書を発行するときにのみ使用されます。

例

次に、DN を指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma,
c="cisco systems, inc.”
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。
ライフタイム	CA 証明書、発行済みの証明書、または CRL のライフタイムを指定します。

サブネット

ネットワーク オブジェクトのネットワークを設定するには、オブジェクト コンフィギュレーション モードで **subnet** コマンドを使用します。コンフィギュレーションからオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

subnet {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}

no subnet {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}

構文の説明

IPv4_address IPv4_mask	IPv4 ネットワーク アドレスとサブネット マスクを、スペースで区切って指定します。
IPv6_address/*IPv6_prefix*	IPv6 ネットワーク アドレスとプレフィックス長を、/ 記号で区切って指定します。スペースは使用しません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
オブジェクト ネットワーク コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

既存のネットワーク オブジェクトを異なる IP アドレスを使用して設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションに置き換わります。

例

次に、サブネット ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network OBJECT_SUBNET
ciscoasa (config-network-object)# subnet 10.1.1.0 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
description	ネットワーク オブジェクトに説明を追加します。
fqdn	完全修飾ドメイン名のネットワーク オブジェクトを指定します。
host	ホスト ネットワーク オブジェクトを指定します。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。
object network	ネットワーク オブジェクトを作成します。
object-group network	ネットワーク オブジェクト グループを作成します。
range	ネットワーク オブジェクトのアドレス範囲を指定します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。

summary-address（インターフェイス）

特定のインターフェイスの EIGRP のサマリーを設定するには、インターフェイス コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスを削除するには、このコマンドの **no** 形式を使用します。

summary-address *as-number addr mask* [*admin-distance*]

no summary-address *as-number addr mask*

構文の説明

as-number	自律システム番号。これは、EIGRP ルーティング プロセスの自律システム番号と同じである必要があります。
addr	サマリー IP アドレス。
mask	IP アドレスに適用されるサブネット マスク。
admin-distance	（任意）集約ルートのアドミニストレーティブ ディスタンス。有効な値は、0 ～ 255 です。指定されていない場合、デフォルト値は 5 です。

デフォルト

デフォルトの設定は次のとおりです。

- EIGRP は、単一のホスト ルートの場合でも、ルートをネットワーク レベルに自動的に集約します。
- EIGRP 集約ルートのアドミニストレーティブ ディスタンスは 5 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

デフォルトでは、EIGRP はサブネット ルートをネットワーク レベルに集約します。自動ルート集約をディセーブルにするには、**no auto-summary** コマンドを使用します。**summary-address** コマンドを使用すると、サブネット ルート集約をインターフェイス単位で手動で定義できます。

例

次の例では、**tag** を 3 に設定してルート集約を設定しています。

```
ciscoasa(config-if)# summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

次の例に、**no** 形式の **summary-address** コマンドをオプションとともに使用して、オプションをデフォルト値に戻す方法を示します。この例では、先の例で 3 に設定された **tag** 値が、**summary-address** コマンドから削除されます。

```
ciscoasa(config-if)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

次の例では、コンフィギュレーションから **summary-address** コマンドを削除しています。

```
ciscoasa(config-if)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
auto-summary	EIGRP ルーティング プロセスのサマリー アドレスを自動的に作成します。

summary-prefix（IPv6 ルータ OSPF）

IPv6 サマリー プレフィックスを設定するには、IPv6 ルータ OSPF コンフィギュレーション モードで **summary-prefix** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

no summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

構文の説明

not-advertise	（オプション）指定されたプレフィックスとマスクのペアに一致するルートを抑制します。このキーワードは OSPFv3 だけに適用されます。
prefix	宛先の IPv6 プレフィックスを指定します。
tag *tag_value*	（オプション）ルート マップを使用して再配布を制御する match 値として使用できるタグ値を指定します。このキーワードは OSPFv3 だけに適用されます。

デフォルト

デフォルトの設定は次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックスとマスクのペアに一致するルートは抑制されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、IPv6 サマリー プレフィックスを設定します。

例

次の例では、サマリー プレフィックス FECO:: /24 が、アドレス FECO::/1 ～ FECO::/24 を含んでいます。アドレス FECO:: /24 のみが外部 LSA でアドバタイズされます。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 172.16.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 のルータ コンフィギュレーション モードを開始します。
redistribute	ある OSPFv3 ルーティング ドメインから別の OSPFv3 ルーティング ドメインへ IPv6 ルートを再配布します。

summary-address（ルータ ISIS）

IS-IS の集約アドレスを作成するには、ルータ ISIS コンフィギュレーション モードで **summary-address** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

summary-address *address mask* [**level-1 | level-1-2 | level-2**] [**tag** *tag-number*] [**metric** *metric-value*]

no summary-address *address mask* [**level-1 | level-1-2 | level-2**] [**tag** *tag-number*] [**metric** *metric-value*]

構文の説明

level-1	（オプション）設定済みアドレスとマスク値を使用して、レベル 1 に再配布されたルートのみが集約されます。
level-1-2	（オプション）ルートをレベル 1 およびレベル 2 IS-IS に再配布するとき、およびレベル 2 IS-IS がレベル 1 をエリアで到達可能なものとしてアドバタイズしたときにサマリー ルートが適用されます。
level-2	（オプション）設定済みアドレスとマスク値を使用して、レベル 1 ルーティングが学習したルートはレベル 2 バックボーンに集約されます。レベル 2 の IS-IS に再配布されたルートもサマライズされます。
address	アドレスの範囲を表すために指定するサマリー アドレス。
mask	サマリー ルートに使用される IP サブネット マスク。
tag *tag-number*	（オプション）サマリー ルートにタグを付けるために使用される整数を指定します。
metric *metric-value*	（オプション）サマリー ルートに適用されるメトリック値を指定します。

コマンド デフォルト

すべてのルートは個別にアドバタイズされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

複数のアドレス グループを特定のレベルに集約できます。他のルーティング プロトコルから学習したルートも集約できます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。このコマンドは、ルーティング テーブルの容量縮小に有効です。

リンクステート パケット（LSP）とリンクステート データベース（LSDB）のサイズも小さくします。また、要約アドバタイズメントは多くの特定ルートによって異なるので、ネットワークの安定にも役立ちます。たいていの場合、1 つのルート フラップが原因で要約アドバタイズメントはフラップしません。

サマリー アドレスを使用する場合の欠点は、他のルートには、個々の宛先すべてに最適なルーティング テーブルを計算するための情報が少なくなることです。

例

次に、IS-IS に Routing Information Protocol（RIP）ルートを再配布する例を示します。RIP ネットワークでは、10.1.1、10.1.2、10.1.3、10.1.4 のような IP ルートがあります次に、10.1.0.0 のみを IS-IS レベル 1 リンクステート プロトコル データ ユニット（PDU）にアドバタイズする例を示します。サマリー アドレスに 100 のタグが付けられ、110 のメトリック値が指定されます。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 01.0000.0000.0001.00
ciscoasa(config-router)# redistribute rip level-1 metric 40
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。

コマンド	説明
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。

コマンド	説明
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

summary-address（ルータ OSPF）

OSPF の集約アドレスを作成するには、ルータ OSPF コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスまたは特定のサマリー アドレス オプションを削除するには、このコマンドの **no** 形式を使用します。

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

構文の説明

addr	アドレス範囲に対して指定されるサマリー アドレスの値。
mask	集約ルートに対して使用される IP サブネット マスク。
not-advertise	（任意）指定されたプレフィックス/マスク ペアと一致するルートを抑制します。
tag *tag_value*	（任意）各外部ルートに付けられた 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効値の範囲は、0 ～ 4294967295 です。

デフォルト

デフォルトの設定は次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックス/マスク ペアと一致するルートは抑制されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

他のルーティング プロトコルから学習したルートをサマライズできます。このコマンドを OSPF に対して使用すると、OSPF 自律システム境界ルータ（ASBR）により、このアドレスの対象となる再配布されるすべてのルートの集約として、1 つの外部ルートがアドバタイズされます。このコマンドでは、OSPF に再配布されている、他のルーティング プロトコルからのルートのみが集約されます。OSPF エリア間のルート集約には **area range** コマンドを使用します。

summary-address コマンドをコンフィギュレーションから削除するには、このコマンドの no 形式を、任意のキーワードまたは引数を指定しないで使用します。コンフィギュレーションの summary コマンドからオプションを削除するには、このコマンドの **no** 形式を使用して、削除するオプションを指定します。詳細については、「例」を参照してください。

例

次の例では、**tag** を 3 に設定してルート集約を設定しています。

```
ciscoasa(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

次の例に、**no** 形式の **summary-address** コマンドをオプションとともに使用して、オプションをデフォルト値に戻す方法を示します。この例では、先の例で 3 に設定された **tag** 値が、**summary-address** コマンドから削除されます。

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

次の例では、コンフィギュレーションから **summary-address** コマンドを削除しています。

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
area range	エリア境界でルートを統合および集約します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf summary-address	各 OSPF ルーティング プロセスのサマリー アドレス設定を表示します。

sunrpc-server

SunRPC サービス テーブルのエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。SunRPC サービス テーブルのエントリをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* **[-** *port* **] timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [*- port]* **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

構文の説明

ifc_name	サーバ インターフェイス名。
ip_addr	SunRPC サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* [- *port*]	SunRPC プロトコルのポート範囲を指定します。
port- *port*	（任意）SunRPC プロトコルのポート範囲を指定します。
protocol tcp	SunRPC トランスポート プロトコルを指定します。
protocol udp	SunRPC トランスポート プロトコルを指定します。
service	サービスを指定します。
service_type	**sunrpcinfo** コマンドで指定した SunRPC サービス プログラム番号を設定します。
timeout *hh:mm:ss*	SunRPC サービス トラフィックへのアクセスが終了するまでのタイムアウト アイドル時間を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

SunRPC サービス テーブルは、timeout で指定された時間、確立された SunRPC セッションに基づいて、SunRPC トラフィックが ASA を通過するのを許可するために使用します。

例

次に、SunRPC サービス テーブルを作成する例を示します。

```
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	ASA からの Sun リモート プロセッサ コール サービスをクリアします。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

support-user-cert-validation

現在のトラストポイントが、リモート ユーザ証明書を発行した CA に対して認証されている場合に、このトラストポイントに基づいてリモート証明書を検証するには、クリプト CA トラストポイント コンフィギュレーション モードで **support-user-cert-validation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

support-user-cert-validation

no support-user-cert-validation

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定では、ユーザ証明書の検証がサポートされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA では、同じ CA に対して 2 つのトラストポイントを保持できます。この場合は、同じ CA から 2 つの異なるアイデンティティ証明書が発行されます。トラストポイントが、この機能をイネーブルにしている別のトラストポイントにすでに関連付けられている CA に対して認証される場合、このオプションは自動的にディセーブルになります。これにより、パス検証パラメータの選択であいまいさが生じないようになります。ユーザが、この機能をイネーブルにした別のトラストポイントにすでに関連付けられている CA に認証されたトラストポイントでこの機能を有効化しようとした場合、アクションは許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central でユーザ検証を受け入れることができるようにする例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# support-user-cert-validation
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。

switchport

インターフェイスをスイッチポートモードに設定するには、インターフェイス コンフィギュレーション モードで **switchport** コマンドを使用します。インターフェイスをファイアウォール モードに設定するには、このコマンドの **no** 形式を使用します。

switchport

no switchport

(注) Firepower 1010 でのみサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

イーサネット 1/2 ～ 1/8 では、このコマンドがデフォルトで有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

各インターフェイスは、ファイアウォール インターフェイスまたはスイッチ ポートのいずれかになるように個別に設定できます。デフォルトでは、イーサネット 1/1 はファイアウォール インターフェイスで、残りのイーサネット インターフェイスはスイッチ ポートとして設定されます。

管理 1/1 インターフェイスをスイッチポートモードに設定することはできません。

このインターフェイスがすでにスイッチポートモードの場合、**switchport** コマンドを入力すると、モードを変更する代わりにスイッチポートパラメータを入力するよう求められます。

例

次に、イーサネット 1/3 および 1/4 をファイアウォールモードに設定する例を示します。

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
forward interface	1 つの VLAN から別の VLAN への転送を無効にします。
interface vlan	Firepower 1010 スイッチポートで使用する VLAN インターフェイスを作成します。
switchport access vlan	アクセスモードのスイッチポートで VLAN を特定します。
switchport mode	スイッチポートをアクセスモードまたはトランクモードに設定します。
switchport trunk allowed vlan	トランクモードのスイッチポートで VLAN を特定します。

sw-module module password-reset

ソフトウェア モジュールのパスワードをデフォルト値にリセットするには、特権 EXEC モードで **sw-module module password-reset** コマンドを使用します。

sw-module module *id* **password-reset**

構文の説明

id	**cxsc** または **ips** のいずれかのモジュール ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。

使用上のガイドライン

パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中はサービスを使用できません。リブートには数分を要する場合があります。**show module** コマンドを実行すると、モジュールの状態をモニタできます。

コマンドは、必ずプロンプトで確認を要求します。コマンドが成功した場合は、それ以上何も出力されません。コマンドが失敗した場合は、障害が発生した理由を示すエラー メッセージが表示されます。

このコマンドは、モジュールがアップ状態である場合にのみ有効です。

デフォルトのパスワードはモジュールによって異なります。

- ASA IPS：ユーザ cisco のデフォルトのパスワードは、**cisco** です。
- ASA CX：ユーザ admin のデフォルトのパスワードは、**Admin123** です。

例

次に、IPS モジュール上のパスワードをリセットする例を示します。

```
ciscoasa# sw-module module ips password-reset
Reset the password on module ips? [confirm] y
```

関連コマンド

コマンド	説明
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reload	モジュール ソフトウェアをリロードします。
sw-module module reset	モジュールをシャットダウンし、リロードします。
sw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

sw-module module recover

ソフトウェア モジュールのリカバリ用ソフトウェア イメージをディスクからロードする場合、またはイメージの場所を設定する場合は、特権 EXEC モードで **sw-module module recover** コマンドを使用します。たとえば、モジュールが現在のイメージをロードできない場合などに、このコマンドを使用してモジュールを回復することが必要になることがあります。

sw-module module *id* **recover** {**boot** | **stop** | **configure image** *path*}

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール
boot	このモジュールの回復を開始し、**configure** 設定に従って回復イメージをダウンロードします。ダウンロード後、モジュールは新しいイメージからリブートします。
configure image *path*	ローカル ディスク上の新しいイメージの場所を設定します（例：disk0:image2）。
stop	リカバリ アクションを停止し、モジュールのイメージ ファイルを削除します。このコマンドは、**sw-module module** *id* **recover boot** コマンドを使用して回復を開始してから 30 秒以内に入力する必要があります。この期間が経過した後で **stop** コマンドを入力すると、モジュールが無応答になるなど、予期しない結果になることがあります。 すでにモジュールが無応答になっている場合、リブートしたり新しいイメージを適用したりするには、停止する必要が生じることがあります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドを使用して、ソフトウェア モジュールをインストールします。このモジュールは、デバイスで設定されていない新しいモジュールである場合と、障害が発生したために再インストールが必要となった既存のモジュールである場合があります。

イメージをインストールする場合は、次のコマンド シーケンスを使用します。

- **sw-module module** *id* **configure image** *path*（ソフトウェア モジュール イメージの disk0 上の場所を指定）。
- **sw-module module** *id* **boot**（該当イメージをブート）。

イメージのブートは、モジュールがアップ、ダウン、無応答、または回復のいずれかの状態である場合にのみ可能です。ステート情報については、**show module** コマンドを参照してください。モジュールがアップ状態でない場合、ASA は強制的にモジュールをシャットダウンします。強制シャットダウンでは、すべてのコンフィギュレーションを含む、古いモジュール ディスク イメージが破壊されます。このため、ディザスタ リカバリ メカニズムとしてのみ使用してください。

show module *id* **recover** コマンドを使用してリカバリ コンフィギュレーションを表示できます。

（注） IPS モジュールの場合、モジュール ソフトウェア内部では、イメージをインストールするために **upgrade** コマンドを使用しないでください。モジュールのインストールおよび初期設定を完了する方法については、各ソフトウェア モジュールの CLI 設定ガイドを参照してください。

例

次に、disk0:image2 からイメージをダウンロードするようにモジュールを設定する例を示します。

```
ciscoasa# sw-module module ips recover configure image disk0:image2
```

次に、モジュールを回復する例を示します。

```
ciscoasa# sw-module module ips recover boot
The module in slot ips will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot ips? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module reset	モジュールをシャットダウンし、リセットを実行します。
sw-module module reload	モジュール ソフトウェアをリロードします。

コマンド	説明
sw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

sw-module module reload

ソフトウェア モジュールのモジュール ソフトウェアをリロードするには、特権 EXEC モードで **sw-module module reload** コマンドを使用します。

sw-module module *id* **reload**

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、モジュールをリロードする前にリセットを実行する **sw-module module reset** コマンドとは異なります。

このコマンドは、モジュールのステータスがアップ状態にある場合だけ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、IPS モジュールをリロードする例を示します。

```
ciscoasa# sw-module module ips reload
Reload module in slot ips? [confirm] y
Reload issued for module in slot ips
%XXX-5-505002: Module in slot ips is reloading.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reset	モジュールをシャットダウンし、リセットを実行します。
sw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

sw-module module reset

モジュールをリセットしてからモジュール ソフトウェアをリロードするには、特権 EXEC モードで **sw-module module reset** コマンドを使用します。

sw-module module *id* **reset**

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

モジュールがアップ状態の場合、**sw-module module reset** コマンドによって、リセットの前にソフトウェアをシャットダウンするように要求されます。

sw-module module recover コマンドを使用してモジュールを回復できます。モジュールが回復状態になっているときに **sw-module module reset** コマンドを入力しても、モジュールは回復プロセスを中断しません。**sw-module module reset** コマンドによって、モジュールのリセットが実行され、リセット後にモジュールの回復が続行します。モジュールがハングした場合は、回復中にモジュールをリセットできます。ハードウェア リセットによって、問題が解決することもあります。

このコマンドは、ソフトウェアのリロードのみを行いリセットは行わない **sw-module module reload** コマンドとは異なります。

このコマンドは、モジュールのステータスがアップ、ダウン、無応答、または回復のいずれかの場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、アップ状態の IPS モジュールをリセットする例を示します。

```
ciscoasa# sw-module module ips reset
The module in slot ips should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot ips? [confirm] y
Reset issued for module in slot ips
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
%XXX-5-505003: Module in slot ips is resetting.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reload	モジュール ソフトウェアをリロードします。
sw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

sw-module module shutdown

モジュール ソフトウェアをシャットダウンするには、特権 EXEC モードで **sw-module module shutdown** コマンドを使用します。

sw-module module *id* **shutdown**

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。

このコマンドは、モジュール ステータスがアップまたは無応答である場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、IPS モジュールをシャットダウンする例を示します。

```
ciscoasa# sw-module module ips shutdown
Shutdown module in slot ips? [confirm] y
Shutdown issued for module in slot ips
ciscoasa#
```

```
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reload	モジュール ソフトウェアをリロードします。
sw-module module reset	モジュールをシャットダウンし、リセットを実行します。
show module	モジュール情報を表示します。

sw-module module uninstall

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールするには、特権 EXEC モードで **sw-module module uninstall** コマンドを使用します。

sw-module module *id* **uninstall**

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、ソフトウェア モジュール イメージおよび関連するコンフィギュレーションを永続的にアンインストールします。

例

次に、IPS モジュール イメージおよびコンフィギュレーションをアンインストールする例を示します。

```
ciscoasa# sw-module module ips uninstall
Module ips will be uninstalled. This will completely remove the
disk image associated with the sw-module including any configuration
that existed within it.

Uninstall module <id>? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reload	モジュール ソフトウェアをリロードします。
sw-module module reset	モジュールをシャットダウンし、リセットを実行します。
show module	モジュール情報を表示します。

switchport

インターフェイスをスイッチポートモードに設定するには、インターフェイス コンフィギュレーション モードで **switchport** コマンドを使用します。インターフェイスをファイアウォール モードに設定するには、このコマンドの **no** 形式を使用します。

switchport

no switchport

(注) Firepower 1010 でのみサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

イーサネット 1/2 ～ 1/8 では、このコマンドがデフォルトで有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

各インターフェイスは、ファイアウォール インターフェイスまたはスイッチ ポートのいずれかになるように個別に設定できます。デフォルトでは、イーサネット 1/1 はファイアウォール インターフェイスで、残りのイーサネット インターフェイスはスイッチ ポートとして設定されます。

管理 1/1 インターフェイスをスイッチポートモードに設定することはできません。

このインターフェイスがすでにスイッチポートモードの場合、**switchport** コマンドを入力すると、モードを変更する代わりにスイッチポートパラメータを入力するよう求められます。

例

次に、イーサネット 1/3 および 1/4 をファイアウォールモードに設定する例を示します。

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
forward interface	1 つの VLAN から別の VLAN への転送を無効にします。
interface vlan	Firepower 1010 スイッチポートで使用する VLAN インターフェイスを作成します。
switchport access vlan	アクセスモードのスイッチポートで VLAN を特定します。
switchport mode	スイッチポートをアクセスモードまたはトランクモードに設定します。
switchport trunk allowed vlan	トランクモードのスイッチポートで VLAN を特定します。

switchport access vlan

アクセスモードのスイッチポートに VLAN を設定するには、インターフェイス コンフィギュレーション モードで **switchport access vlan** コマンドを使用します。デフォルトの VLAN 1 に戻すには、このコマンドの **no** 形式を使用します。

switchport access vlan *number*

no switchport access vlan *number*

(注) Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

vlan *number*	このスイッチ ポートを割り当てる VLAN ID を指定します。VLAN ID は、1 ～ 4070（Firepower 1010）または 4090（ASA 5505）の範囲で指定します。

デフォルト

Firepower 1010：デフォルトでは、イーサネット 0/1 ～ 0/7 が VLAN 1 に割り当てられ、イーサネット 0/0 が VLAN 2 に割り当てられます。

Firepower 1010：デフォルトでは、イーサネット 1/2 ～ 1/8 のスイッチポートがアクセスモードとなり、VLAN 1 に割り当てられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

アクセス ポートは、タグなしのトラフィックのみを受け入れます。ASA は、指定した VLAN を使用してスイッチポートに入るトラフィックにタグを付け、同じ VLAN 上の他のアクセスポートまたはトランクポートにトラフィックを転送できるようにします。VLAN タグは、別のアクセスポートを出力すると削除されますが、トランクポートを出力しても保持されます。

(注) ASA は、ネットワーク内のループ検出に使用されるスパニングツリープロトコルをサポートしていません。したがって、ASA との接続はいずれもネットワークループ内で終わらないようにする必要があります。

ASA 5505

トランスペアレント ファイアウォール モードでは、ASA 5505 基本ライセンスはアクティブ VLAN を 2 つ、Security Plus ライセンスは 3 つ設定できます。そのうちの 1 つは、フェールオーバー用です。

ルーテッドモードでは、ASA 5505 の基本ライセンスで最大 3 つのアクティブ VLAN と Security Plus ライセンスで最大 20 のアクティブ VLAN を設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。

例

次に、5 つの ASA 5505 物理インターフェイスを 3 つの VLAN インターフェイスに割り当てる例を示します。

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport	インターフェイスをスイッチポートモードに設定します。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport mode

スイッチポートの VLAN をアクセスモード(デフォルト)またはトランクモードのいずれかに設定するには、インターフェイス コンフィギュレーション モードで **switchport mode** コマンドを使用します。デフォルトのアクセスモードに戻すには、このコマンドの **no** 形式を使用します。

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

(注) Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

アクセス	スイッチ ポートをアクセス モードに設定します。このモードでは、スイッチ ポートで 1 つの VLAN のみのトラフィックを渡すことができます。タグなしパケットのみが許可されます。パケットがタグ付きでスイッチ ポートに入ると、パケットはドロップされます。パケットは、802.1Q VLAN タグなしでスイッチ ポートから出ます。
トランク	スイッチ ポートをトランク モードに設定します。そのため、複数の VLAN のトラフィックを渡すことができます。タグ付きのパケットとタグなしパケットの両方が許可されます。パケットは、802.1Q VLAN タグ付きでスイッチ ポートから出ます。パケットがタグなしでスイッチポートに入ると、ネイティブ VLAN に割り当てられます。

デフォルト

デフォルトでは、モードはアクセスです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
7.2(2)	1 つのトランクに制限されず、複数のトランク ポートを設定できるようになりました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

モードをアクセスモードに設定した後、**switchport vlan access** コマンドを使用して VLAN を識別します。

モードをトランクモードに設定した後、**switchport trunk allowed vlan** コマンドを使用して、複数の VLAN をトランクに割り当てます。モードをトランクモードに設定したが、まだ **switchport trunk allowed vlan** コマンドを設定していない状態では、スイッチポートが「回線プロトコルダウン」状態になり、トラフィック転送に参加できません。ASA 5505 でトランクモードが使用できるのは、Security Plus ライセンスだけです。

例

次に、VLAN 100 に割り当てられたアクセス モードのスイッチ ポートおよび VLAN 200 および 300 に割り当てられたトランク モードのスイッチ ポートを設定する例を示します。

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200,300
ciscoasa(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport	インターフェイスをスイッチポートモードに設定します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport monitor

SPAN スイッチポートモニタリングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **switchport monitor** コマンドを使用します。このコマンドを入力する対象のポート（宛先ポートと呼ばれる）では、指定した送信元ポートで送受信されるすべてのパケットのコピーを受信します。SPAN 機能を使用すると、トラフィックをモニタできるように、スニファを宛先ポートに接続できます。このコマンドを複数回入力して、複数の送信元ポートを指定できます。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。送信元ポートのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport monitor *source_port* [**tx** | **rx** | **both**]

no switchport monitor *source_port* [**tx** | **rx** | **both**]

（注） ASA 5505 でのみサポートされています。

構文の説明

both	（任意）送信トラフィックと受信トラフィックの両方をモニタすることを指定します。**both** がデフォルトです。
rx	（任意）受信トラフィックのみをモニタすることを指定します。
source_port	モニタするポートを指定します。任意のイーサネット ポートおよび VLAN インターフェイス間でトラフィックを渡す Internal-Data0/1 バックプレーン ポートを指定できます。Internal-Data0/1 ポートはギガビット イーサネット ポートであるため、ファスト イーサネット宛先ポートをトラフィックによって過負荷にする場合があります。Internal-Data0/1 ポートは注意してモニタしてください。
tx	（任意）送信トラフィックのみをモニタすることを指定します。

デフォルト

モニタするトラフィックのデフォルトのタイプは **both** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

SPAN をイネーブルにしない場合、スニファをスイッチ ポートの 1 つに接続すると、そのポートで送受信されるトラフィックのみがキャプチャされます。複数のポートで送受信されるトラフィックをキャプチャするには、SPAN をイネーブルにし、モニタするポートを指定する必要があります。

ネットワーク ループになる可能性があるため、SPAN 宛先ポートを別のスイッチに接続するときは注意してください。

例

次に、イーサネット 0/0 ポートとイーサネット 0/2 ポートをモニタする宛先ポートとして、イーサネット 0/1 ポートを設定する例を示します。

```
ciscoasa(config)# interface ethernet 0/1
ciscoasa(config-if)# switchport monitor ethernet 0/0
ciscoasa(config-if)# switchport monitor ethernet 0/2
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。

switchport protected

スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信しないようにするには、インターフェイス コンフィギュレーション モードで **switchport protected** コマンドを入力します。この機能により、あるスイッチ ポートが侵害された場合に、VLAN 上の他のスイッチ ポートに対して強固なセキュリティを提供します。保護されたモードをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport protected

no switchport protected

(注) Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、インターフェイスは保護されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに **switchport protected** コマンドを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

保護されていないポートとの通信は、このコマンドによって制限されません。

例

次に、7 つのスイッチ ポートを設定する例を示します。イーサネット 0/4、0/5、および 0/6 は DMZ ネットワークに割り当てられ、相互から保護されます。

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/5
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/6
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport trunk

VLAN をトランクポートに割り当てるには、インターフェイス コンフィギュレーション モードで **switchport trunk** コマンドを使用します。VLAN をトランクから削除するには、このコマンドの **no** 形式を使用します。

switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

no switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

(注) Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

allowed vlans *vlan_range*	トランク ポートに割り当てることができる 1 つ以上の VLAN を指定します。VLAN ID は、1 ～ 4070（Firepower 1010）または 4090（ASA 5505）の範囲で指定します。 *vlan_range* は、次のいずれかの方法で指定できます。 • 単一の番号（n） • 範囲（n-x） 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。 5,7-10,13,45-100 カンマの代わりにスペースを入力できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。 このコマンドにネイティブ VLAN を含めても無視されます。トランクポートは、ネイティブ VLAN トラフィックをポートから送信するときに、常に VLAN タグを削除します。また、まだネイティブ VLAN タグが付いているトラフィックを受信しません。
native vlan *vlan*	ネイティブ VLAN をトランクに割り当てます。トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、ASA が正しいスイッチポートにトラフィックを転送したり、別のファイアウォール インターフェイスにルーティングしたりできるようにします。ASA は、トランクポートからネイティブ VLAN ID トラフィックを送信する際に VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランク ポートに同じネイティブ VLAN を設定してください。 各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

デフォルト

デフォルトでは、VLAN はトランクに割り当てられていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
7.2(2)	このコマンドは、スイッチ ポートごとに 4 つ以上の VLAN を許可するように変更されました。また、1 つのみに制限されず、複数のトランク ポートを設定できるようになりました。このコマンドで、VLAN ID を区切るためにスペースではなくカンマも使用されます。
7.2(4)/8.0(4)	**native vlan** キーワードを使用するネイティブ VLAN サポートが追加されました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

スイッチ ポートで複数の VLAN を渡すトランク ポートを作成する場合は、**switchport mode trunk** コマンドを使用してモードをトランク モードに設定してから、**switchport trunk** コマンドを使用して VLAN をトランクに割り当てます。このスイッチ ポートに少なくとも 1 つの VLAN を割り当てるまで、このスイッチ ポートでトラフィックを渡すことはできません。モードをトランク モードに設定し、**switchport trunk allowed vlan** コマンドを設定していない状態では、スイッチ ポートは「回線プロトコル ダウン」状態になり、トラフィック転送に参加できません。

ASA 5505

トランク モードが使用できるのは Security Plus ライセンスだけです。

(注) このコマンドにはバージョン 7.2(1) との下位互換性はありません。VLAN を区切るカンマは 7.2(1) では認識されません。ダウングレードする場合は、VLAN をスペースで区切り、3 つの VLAN という制限を超えないようにしてください。

例

次に、7 つの VLAN インターフェイスを設定する例を示します。**failover lan** コマンドを使用して設定するフェールオーバー インターフェイスが含まれています。VLAN 200、201、および 202 は、イーサネット 0/1 でトランキングされています。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

```
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 201
ciscoasa(config-if)# nameif dept1
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 202
ciscoasa(config-if)# nameif dept2
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.3.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# failover lan faillink vlan500
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200-202
ciscoasa(config-if)# switchport trunk native vlan 5
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。

コマンド	説明
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。

synack-data

データが含まれる TCP SYNACK パケットのアクションを設定するには、tcp マップ コンフィギュレーション モードで **synack-data** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

synack-data {**allow** | **drop**}

no synack-data

構文の説明

allow	データが含まれる TCP SYNACK パケットを許可します。
drop	データが含まれる TCP SYNACK パケットをドロップします。

デフォルト

デフォルト アクションでは、データが含まれる TCP SYNACK パケットをドロップします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが追加されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **synack-data**：tcp マップ コンフィギュレーション モードでは、**synack-data** などの数多くのコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、データが含まれる TCP SYNACK パケットを許可するようにASAを設定する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# synack-data allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシー内でトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

synchronization

BGP と内部ゲートウェイ プロトコル(IGP)システム間の同期をイネーブルにするには、アドレス ファミリ コンフィギュレーション モードで **synchronization** コマンドを使用します。Cisco IOS ソフトウェアが IGP を待機せずにネットワーク ルートをアドバタイズできるようにするには、このコマンドの **no** 形式を使用します。

synchronization

no synchronization

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレスファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。デフォルトでは BGP と IGP 間の同期はオフになっており、Cisco IOS ソフトウェアが IGP を待機せずにネットワーク ルートをアドバタイズできるようになっています。この機能により、自律システム内のルータおよびアクセス サーバは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。

自律システム内のルータが BGP を実行していない場合は、**synchronization** コマンドを使用します。

例

次に、アドレス ファミリ コンフィギュレーション モードで同期をイネーブルにする例を示します。ルータは、ルートを外部にアドバタイズする前に、IGP 内のネットワーク ルートを検証します。

```
ciscoasa(config)# router bgp 65120
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# synchronization
```

syn-data

データが含まれる SYN パケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

構文の説明

allow	データが含まれる SYN パケットを許可します。
drop	データが含まれる SYN パケットをドロップします。

デフォルト

デフォルトでは、SYN データが含まれるパケットは許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用して、SYN パケット内にデータが含まれるパケットをドロップします。

TCP の仕様によると、TCP 実装は SYN パケット内に含まれているデータを受け入れる必要があります。これは微妙であいまいな点であるため、一部の実装ではこのことが正しく処理されない場合があります。不適切なエンドシステム実装などの挿入攻撃に対する脆弱性を回避するために、SYN パケット内にデータが含まれるパケットをドロップすることを選択できます。

例

次に、データが含まれる SYN パケットをすべての TCP フローでドロップする例を示します。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# syn-data drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

sysopt connection permit-vpn

VPN トンネルを介して ASA に入り復号化されるトラフィックに対して、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用して、トラフィックがインターフェイス アクセス リストをバイパスできるようにします。グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection permit-vpn

no sysopt connection permit-vpn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、デフォルトでイネーブルになりました。また、インターフェイス アクセス リストのみがバイパスされます。グループ ポリシーまたはユーザ単位のアクセス リストは有効なままです。
7.1(1)	このコマンドは、**sysopt connection permit-ipsec** から変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

デフォルトでは、ASA によって、VPN トラフィックが ASA のインターフェイスで終端することが許可されています。IKE または ESP（またはその他のタイプの VPN パケット）をインターフェイス アクセス リストで許可する必要はありません。デフォルトでは、復号化された VPN パケットのローカル IP アドレスのインターフェイス アクセス リストも必要ありません。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、コンフィギュレーションが簡略化され、ASA のパフォーマンスはセキュリティ リスクを負うことなく最大化されます（グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます）。

no sysopt connection permit-vpn コマンドを入力して、インターフェイス アクセス リストをローカル IP アドレスに適用できます。アクセス リストを作成してインターフェイスに適用するには、**access-list** コマンドおよび **access-group** コマンドを参照してください。アクセス リストは、ローカル IP アドレスに適用され、VPN パケットが復号化される前に使用された元のクライアント IP アドレスには適用されません。

例

次に、復号化された VPN トラフィックがインターフェイス アクセス リストに従うようにする例を示します。

```
ciscoasa(config)# no sysopt connection permit-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection preserve-vpn-flows

トンネルのドロップおよび回復後のタイムアウト期間内に、ステートフル(TCP)トンネル IPSec LAN-to-LAN トラフィックを保持して再開するには、**sysopt connection preserve-vpn-flows** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection preserve-vpn-flows

no sysopt connection preserve-vpn-flows

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

永続的 IPSec トンネル フロー機能がイネーブルの場合、タイムアウト ウィンドウ内にトンネルが再作成される限り、セキュリティ アプライアンスで元のフロー内の状態情報にアクセスできるため、データは正常に流れ続けます。

このコマンドでは、ネットワーク拡張モードを含め、IPSec LAN-to-LAN トンネルのみがサポートされます。AnyConnect/SSL VPN または IPSec リモートアクセス トンネルはサポートされません。

例

次に、トンネルがドロップされ、タイムアウト期間内に再確立された後、トンネルの状態情報が保持されてトンネル IPSec LAN-to-LAN VPN トラフィックが再開されることを指定する例を示します。

```
ciscoasa(config)# no sysopt connection preserve-vpn-flows
```

この機能がイネーブルかどうかを確認するには、sysopt に対して show run all コマンドを入力します。

```
ciscoasa(config)# show run all sysopt
```

結果の例は次のとおりです。説明のために、これ以降のすべての例では、preserve-vpn-flows の項目は太字になっています。

```
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

既存の VPN フローを再分類するには、グローバル コンフィギュレーション モードで **sysopt connection reclassify-vpn** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection reclassify-vpn

no sysopt connection reclassify-vpn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

VPN トンネルがアップになると、このコマンドによって既存の VPN フローは再分類され、暗号化が必要なフローは分解されて再作成されます。

このコマンドは、LAN-to-LAN およびダイナミック VPN についてのみ適用されます。このコマンドは EZVPN または VPN クライアント接続には影響しません。

例

次に、VPN 再分類をイネーブルにする例を示します。

```
ciscoasa(config)# sysopt connection reclassify-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-vpn	インターフェイスのアクセス リストを確認することなく、IPsec トンネルを経由してきたパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection tcpmss

通過トラフィックの最大 TCP セグメント サイズが設定した値を超えないようにし、指定したサイズ未満にならないようにするには、グローバル コンフィギュレーション モードで **sysopt connection tcpmss** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

構文の説明

bytes	最大 TCP セグメント サイズをバイト単位で設定します(48 ～任意の最大値)。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、*bytes* を 0 に設定します。 **minimum** キーワードの場合、*bytes* は許可される最も小さい最大値を表します。
minimum	最大セグメント サイズを上書きし、*bytes* 未満にならないようにします(48 ～ 65535 バイト)。この機能は、デフォルトでディセーブルです(0 に設定)。

デフォルト

デフォルトでは、ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

minimum 機能は、デフォルトでディセーブルです(0 に設定)。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

最大セグメント サイズ(TCP MSS)とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

通過トラフィックの TCP MSS を ASA に設定できます。デフォルトでは、最大 TCP MSS は 1380 バイトに設定されます。この設定は、ASA が IPsec VPN カプセル化のパケット サイズを追加する必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、ASA の最大 TCP MSS を無効にする必要があります。

最大 TCP MSS を設定している場合、接続のいずれかのエンドポイントが ASA に設定された値を超える TCP MSS を要求すると、ASA は要求パケット内の TCP MSS を ASA の最大サイズで上書きします。ホストまたはサーバが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイト(IPv4)または 1220 バイト(IPv6)を想定しますが、パケットは変更しません。たとえば、MTU を デフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。ASA の最大 TCP MSS が 1380(デフォルト)の場合は、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380 バイトのペイロードを含むパケットを送信します。ASA は、最大 120 バイトのヘッダーをパケットに追加しても、1500 バイトの MTU サイズに適応することができます。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、ASA は値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含め、to-the-box トラフィックの場合、この設定は適用されません。ASA は MTU を使用して、TCP MSS を導き出します。MTU - 40(IPv4)または MTU - 60(IPv6)となります。

デフォルトでは TCP MSS は、ASA が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。ASA が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして ASA を使用しない場合は、TCP MSS 設定を変更する必要があります。次のガイドラインを参照してください。

- 通常のトラフィック:TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。通常、接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。
- IPv4 IPsec エンドポイント トラフィック:最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック:最大 TCP MSS を MTU - 140 に設定します。

例

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、非 VPN トラフィックの TCP MSS をディセーブルにします(TCP MSS を 0 に設定、すなわち無制限とすることによって行います)。

```
ciscoasa(config)# jumbo frame-reservation
ciscoasa(config)# mtu inside 9198
ciscoasa(config)# mtu outside 9198
ciscoasa(config)# sysopt connection tcpmss 0
```

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、VPN トラフィックの TCP MSS を 9078 に変更します(MTU から 120 を差し引きます)。

```
ciscoasa(config)# jumbo frame-reservation
ciscoasa(config)# mtu inside 9198
ciscoasa(config)# mtu outside 9198
ciscoasa(config)# sysopt connection tcpmss 9078
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPsec トンネルからのすべてのパケットを許可します。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection timewait

各 TCP 接続において、最後の通常の TCP クローズ ダウン シーケンスの後に、少なくとも 15 秒の短い TIME_WAIT 状態が強制的に維持されるようにするには、グローバル コンフィギュレーション モードで **sysopt connection timewait** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合に、この機能を使用することを推奨します。

sysopt connection timewait

no sysopt connection timewait

(注) FIN_WAIT2 状態で受信した RST パケット（通常の TCP クローズダウン シーケンスではなく）は、15 秒の遅延もトリガーします。ASA では、接続の最後のパケット（FIN/ACK または RST）を受信した後、接続を 15 秒間保持します。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA のデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後で接続が解放されます。この即時解放ヒューリスティックにより、ASA では、標準クローズ シーケンスと呼ばれる最も一般的なクロージング シーケンスに基づいて、高い接続レートを維持できます。ただし、一方の端が閉じ、もう一方の端が確認応答してから独自のクロージング シーケンスを開始する標準クローズ シーケンスとは異なり、同時クローズでは、トランザクションの両端がクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、即時解放によって接続の一方の側で CLOSING 状態が保持されます。多くのソケットを CLOSING 状態にすると、エンド ホストのパフォーマンスが低下する可能性があります。たとえば、一部の WinSock メインフレーム クライアントはこの動作を示し、メインフレーム サーバのパフォーマンスを低下させることが知られています。**sysopt connection timewait** コマンドを使用すると、同時クローズ ダウン シーケンスが完了するためのウィンドウが作成されます。

例

次に、timewait 機能をイネーブルにする例を示します。

```
ciscoasa(config)# sysopt connection timewait
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPsec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。

sysopt noproxyarp

インターフェイスで NAT グローバル アドレスまたは VPN クライアント アドレスに対するプロキシ ARP をディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt noproxyarp** コマンドを使用します。プロキシ ARP を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

構文の説明

interface_name	プロキシ ARP をディセーブルにするインターフェイス名。

デフォルト

プロキシ ARP は、デフォルトでイネーブルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドは、VPN クライアント アドレスが内部ネットワークと重複するときに、VPN プロキシ ARP に影響を及ぼすように拡張されました。

使用上のガイドライン

既存のネットワークと重なる VPN クライアント アドレス プールがある場合、ASA は、デフォルトにより、すべてのインターフェイス上でプロキシ ARP を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターン トラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP が不要なインターフェイスに対して **sysopt noproxyarp** コマンドを入力する必要があります。

まれに、NAT グローバル アドレスに対してプロキシ ARP をディセーブルにする場合があります。

ホストによって IP トラフィックが同じイーサネット ネットワーク上の別のデバイスに送信される場合、ホストではそのデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが IP アドレスを所有していなくても、その固有の MAC アドレスで ARP 要求に応答する場合に使用します。NAT を設定し、ASA のインターフェイスと同じネットワーク上にあるグローバル アドレスを指定すると、ASA によってプロキシ ARP が使用されます。トラフィックがホストにアクセスできる唯一の方法は、ASA でプロキシ ARP が使用されている場合、ASA の MAC アドレスが宛先グローバル アドレスに割り当てられていると主張することです。

例

次に、内部インターフェイスでプロキシ ARP をディセーブルにする例を示します。

```
ciscoasa(config)# sysopt noproxyarp inside
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に合わせて DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS A レコード アドレスの変更をディセーブルにします。

sysopt radius ignore-secret

RADIUS アカウンティング応答内の認証キーを無視するには、グローバル コンフィギュレーション モードで **sysopt radius ignore-secret** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。一部の RADIUS サーバとの互換性のために、このキーを無視する必要がある場合があります。

sysopt radius ignore-secret

no sysopt radius ignore-secret

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

一部の RADIUS サーバでは、アカウンティング確認応答内のオーセンティケータ ハッシュにこのキーが含まれていません。この使用上の注意により、ASA でアカウンティング要求を継続的に再送信する場合があります。**sysopt radius ignore-secret** コマンドを使用して、これらの確認応答内のキーを無視し、再送信の問題を回避します（ここで示すキーは、**aaa-server host** コマンドで設定するものと同じです）。

例

次に、アカウンティング応答内の認証キーを無視する例を示します。

```
ciscoasa(config)# sysopt radius ignore-secret
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバを指定します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。

sysopt traffic detailed-statistics

変更されたトラフィック システム オプションについて秒単位でプロトコルごとの詳細な統計情報を計算するには、グローバル コンフィギュレーション モードで **sysopt traffic detailed-statistics** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt traffic detailed-statistics

no sysopt traffic detailed-statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

sysopt traffic detailed-statistics コマンドを使用して、変更されたトラフィック システム オプションについて秒単位でプロトコルごとに詳細な統計情報を計算できます。

例

次に、変更されたトラフィック システム オプションの詳細な統計情報を表示する例を示します。

```
ciscoasa(config)# sysopt traffic detailed-statistics
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。