CHAPTER 3

acl-netmask-convert コマンド～ auto-update timeout コマンド

acl-netmask-convert

RADIUS サーバから受信したダウンロード可能な ACL 内のネットマスクをセキュリティ アプライアンスでどのように扱うかを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **acl-netmask-convert** コマンドを使用します。このモードには、**aaa-server host** コマンドを使用してアクセスできます。指定したセキュリティ アプライアンスの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。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

構文の説明

auto-detect	セキュリティ アプライアンスは、使用されているネットマスク表現のタイプを判断しようとします。ワイルドカード ネットマスク表現を検出した場合は、標準ネットマスク表現に変換します。このキーワードの詳細については、「使用上のガイドライン」を参照してください。
standard	セキュリティ アプライアンスは、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。ワイルドカード ネットマスク表現からの変換は実行されません。
wildcard	セキュリティ アプライアンスは、RADIUS サーバから受信したダウンロード可能な ACL にワイルドカード ネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

デフォルト

デフォルトでは、ワイルドカード ネットマスク表現からの変換は実行されません。

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	透過	シングル	コンテキスト	システム
AAA サーバ コンフィギュレーション ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

RADIUS サーバから提供されるダウンロード可能な ACL にワイルドカード形式のネットマスクが含まれている場合は、wildcard または auto-detect キーワードを指定して **acl-netmask-convert** コマンドを使用します。セキュリティ アプライアンスは、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると想定します。一方、Cisco VPN 3000 シリーズ コンセントレータは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカード ネットマスク表現が含まれていると想定しま

す。ワイルドカード マスクでは、無視するビット位置に 1、照合するビット位置に 0 が配置されます。**acl-netmask-convert** コマンドを使用すると、このような相違が RADIUS サーバ上のダウンロード可能な ACL の設定方法に与える影響を最小限に抑えることができます。

RADIUS サーバの設定方法が不明な場合は、**auto-detect** キーワードが役立ちます。ただし、「穴」があるワイルドカード ネットマスク表現は、正しく検出および変換できません。たとえば、ワイルドカード ネットマスク 0.0.255.0 は、第 3 オクテットに任意の値を許可し、Cisco VPN 3000 シリーズ コンセントレータでは有効に使用できます。ただし、セキュリティ アプライアンスでは、この表現をワイルドカード ネットマスクとして検出できません。

例

次に、ホスト「192.168.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、ダウンロード可能な ACL のネットマスクの変換をイネーブルにして、タイムアウトを 9 秒、再試行間隔を 7 秒、認証ポートを 1650 に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# acl-netmask-convert wildcard
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドまたは ASDM ユーザ認証により指定されたサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
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。

action

アクセス ポリシーをセッションに適用するか、またはセッションを終了するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **action** コマンドを使用します。

セッションをリセットしてアクセス ポリシーをセッションに適用するには、このコマンドの **no** 形式を使用します。

action {continue | terminate}

no action {continue | terminate}

構文の説明

continue	アクセス ポリシーをセッションに適用します。
terminate	接続を切断します。

デフォルト

デフォルト値は continue 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	透過	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

選択したすべての DAP レコードでセッションにアクセス ポリシーを適用するには、**continue** キーワードを使用します。選択した DAP レコードのいずれかで接続を切断するには、**terminate** キーワードを使用します。

例

次に、Finance という DAP ポリシーのセッションを切断する例を示します。

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# action terminate
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

action-uri

Web サーバの URI を指定して、シングル サインオン認証用のユーザ名とパスワードを受信するには、AAA サーバ ホスト コンフィギュレーション モードで **action-uri** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。URI パラメータ値をリセットするには、このコマンドの **no** 形式を使用します。

action-uri *string*

no action-uri

（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	認証プログラムの URI。複数行に入力できます。各行の最大文字数は 255 です。URI 全体の最大文字数は、2048 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

Uniform Resource Identifier（URI; ユニフォーム リソース識別子）は、インターネット上のコンテンツの位置を特定するコンパクトなストリングです。これらのコンテンツには、テキスト ページ、ビデオ クリップ、サウンド クリップ、静止画、動画、プログラムなどがあります。URI の最も一般的な形式は、Web ページ アドレスです。Web ページ アドレスは、URI の特定の形式またはサブセットで、URL と呼ばれます。

セキュリティ アプライアンスの WebVPN サーバは、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。これを行うには、HTTP POST 要求を使用して、認証 Web サーバ上のアクション URI にユーザ名とパスワードを渡すようにセキュリティ アプライアンスを設定します。**action-uri** コマンドでは、セキュリティ アプライアンスが POST 要求を送信する Web サーバ上の認証プログラムの場所と名前を指定します。

認証 Web サーバ上のアクション URI を見つけるには、ブラウザで直接 Web サーバのログイン ページに接続します。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバのアクション URI です。

入力しやすいように、URI は連続する複数の行に入力できるようになっています。各行は入力と同時にセキュリティ アプライアンスによって連結され、URI が構成されます。action-uri 行の 1 行あたりの最大文字数は 255 文字ですが、それよりも少ない文字を各行に入力できます。

（注） ストリングに疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次に、www.example.com の URI を指定する例を示します。

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

```
hostname(config)# aaa-server testgrp1 host www.example.com
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
hostname(config-aaa-server-host)#
```

（注） アクション URI にホスト名とプロトコルを含める必要があります。上記の例では、これらは URI の最初にある http://www.example.com に含まれています。

関連コマンド

コマンド	説明
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	SSO サーバとの交換に使用する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。
start-url	プリログイン クッキーを取得する URL 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。

activation-key

セキュリティ アプライアンス のアクティベーション キーを変更し、セキュリティ アプライアンス上で運用されているアクティベーション キーを、セキュリティ アプライアンスのフラッシュ メモリに非表示のファイルとして保存されているアクティベーション キーと比較してチェックするには、グローバル コンフィギュレーション モードで **activation-key** コマンドを使用します。セキュリティ アプライアンスで実行されている、指定したアクティベーション キーを無効にするには、このコマンドの **no** 形式を使用します。

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

no activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

構文の説明

activation-key-four-tuple	アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。
activation-key-five-tuple	アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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 モード	•	•	•		•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

各要素の間にスペースを 1 つ入れて、4 つの要素で構成される 16 進数文字列として *activation-key-four-tuple* を入力します。または、各要素の間にスペースを 1 つ入れて、5 つの要素で構成される 16 進数文字列として、*activation-key-five-tuple* を入力します。次に例を示します。

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。

キーはコンフィギュレーション ファイルに保存されず、シリアル番号に関連付けられます。

例

次に、セキュリティ アプライアンスのアクティベーション キーを変更する例を示します。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

関連コマンド

コマンド	説明
show activation-key	アクティベーション キーを表示します。

activex-relay

WebVPN セッションの ActiveX コントロールをイネーブルまたはディセーブルにするには、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 **activex-relay** コマンドを使用します。デフォルトのグループ ポリシーから **activex-relay** 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。

activex-relay {**enable | disable**}

no activex-relay

構文の説明

enable	WebVPN セッションの ActiveX をイネーブルにします。
disable	WebVPN セッションの ActiveX をディセーブルにします。

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

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

activex-relay enable コマンドを使用すると、ユーザは WebVPN ブラウザから ActiveX コントロールを起動できます。これらのアプリケーションでは、WebVPN セッションを使用して ActiveX コントロールをダウンロードおよびアップロードします。ActiveX リレーは、WebVPN セッションが閉じるまで有効です。

例

次のコマンドは、特定のグループ ポリシーに関連付けられている WebVPN セッションの ActiveX コントロールをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

次のコマンドは、特定のユーザ名に関連付けられている WebVPN セッションの ActiveX コントロールをディセーブルにします。

```
hostname(config-username-policy)# webvpn
```

```
hostname(config-username-webvpn)# activex-relay disable
hostname(config-username-webvpn)
```

address-pool（トンネル グループ一般属性モード）

アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定するには、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 **address-pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface name	（任意）アドレス プールに使用する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	透過	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	•	—	•	—	—

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

これらのコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスが指定されていない場合、コマンドは明示的に参照されていないインターフェイスすべてに対してデフォルトを指定します。

グループ ポリシーの **address-pools** コマンドによるアドレス プール設定は、トンネル グループの **address-pool** コマンドによるローカル プール設定を上書きします。

プールの指定順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、設定トンネル一般コンフィギュレーション モードで、IPSec リモート アクセス トンネル グループ テスト用にアドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定する例を示します。

```
hostname(config)# tunnel-group test type remote-access
hostname(config)# tunnel-group test general
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ip local pool	VPN リモート アクセス トンネルに使用する IP アドレス プールを設定します。
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。
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-map default-group	**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。

address-pools（グループ ポリシー属性コンフィギュレーション モード）

アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定するには、グループ ポリシー属性コンフィギュレーション モードで **address-pools** コマンドを使用します。グループ ポリシーから属性を削除し、別のグループ ポリシー ソースからの継承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。

address-pools value *address_pool1* [*...address_pool6*]

no address-pools value *address_pool1* [*...address_pool6*]

address-pools none

no address-pools none

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
none	アドレス プールを設定しないことを指定し、他のグループ ポリシーからの継承をディセーブルにします。
value	アドレスの割り当てに使用する最大 6 個のアドレス プールのリストを指定します。

デフォルト

デフォルトでは、アドレス プールの属性は継承を許可します。

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	透過	シングル	コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

このコマンドによるアドレス プール設定は、グループ内のローカル プール設定を上書きします。ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。

プールの指定順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

address-pools none コマンドは、この属性が他のポリシー（DefaultGrpPolicy など）から継承されないようにします。**no address pools none** コマンドは、**address-pools none** コマンドをコンフィギュレーションから削除して、デフォルト値（継承の許可）に戻します。

例

次に、GroupPolicy1 の設定一般コンフィギュレーション モードで、アドレスをリモート クライアントに割り当てるために使用するアドレス プールのリストとして pool_1 および pool_20 を設定する例を示します。

```
hostname(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
hostname(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# address-pools value pool_1 pool_20
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
ip local pool	VPN グループ ポリシーで使用する IP アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループ ポリシーをクリアします。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

admin-context

システム コンフィギュレーションの管理コンテキ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 **admin-context** コマンドを使用します。システム コンフィギュレーションには、システム自体のネットワーク インターフェイスまたはネットワーク設定は含まれません。代わりに、システムは、ネットワーク リソースにアクセスする必要がある場合に（セキュリティ アプライアンス ソフトウェアをダウンロードしたり、管理者に対してリモート アクセスを許可する場合など）、管理コンテキストとして指定されたコンテキストのいずれかを使用します。

admin-context *name*

構文の説明

name	名前を最大 32 文字のストリングで設定します。コンテキストをまだ定義していない場合は、まずこのコマンドで管理コンテキスト名を指定します。次に、**context** コマンドを使用して最初に追加するコンテキストを、指定した管理コンテキスト名にする必要があります。 この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

デフォルト

マルチ コンテキスト モードの新しいセキュリティ アプライアンスの場合、管理コンテキスト名は「admin」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	透過	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	•	•	—	—	•

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

コンテキスト コンフィギュレーションが内部フラッシュ メモリにある限り、任意のコンテキストを管理コンテキストに設定できます。

現在の管理コンテキストを削除するには、**clear configure context** コマンドを使用してすべてのコンテキストを削除する必要があります。

例

次に、管理コンテキストを「administrator」に設定する例を示します。

```
hostname(config)# admin-context administrator
```

関連コマンド

コマンド	説明
clear configure context	システム コンフィギュレーションからすべてのコンテキストを削除します。
context	システム コンフィギュレーションにコンテキストを設定し、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 admin-context	現在の管理コンテキスト名を表示します。

alias

アドレスを手動で変換し、DNS 応答を変更するには、グローバル コンフィギュレーション モードで **alias** コマンドを使用します。**alias** 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。

alias (*interface_name***)** *real_ip mapped_ip* [*netmask*]

no alias (*interface_name***)** *real_ip mapped_ip* [*netmask*]

構文の説明

(*interface_name***)**	マッピングされた IP アドレス宛てのトラフィック用の入力インターフェイス（またはマッピングされた IP アドレスからのトラフィック用の出力インターフェイス）の名前を指定します。コマンドにカッコを含めてください。
mapped_ip	実際の IP アドレスの変換先 IP アドレスを指定します。
netmask	（任意）両方の IP アドレスのサブネット マスクを指定します。ホスト マスクの場合は、**255.255.255.255** と入力します。
real_ip	実際の 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	透過	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	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドの機能は、外部 NAT コマンド（**dns** キーワードを指定した **nat** コマンドや **static** コマンド）に置き換えられています。**alias** コマンドの代わりに、外部 NAT コマンドを使用することを推奨します。

宛先アドレスに対してアドレス変換を実行するには、このコマンドを使用します。たとえば、ホストがパケットを 209.165.201.1 に送信する場合は、**alias** コマンドを使用して、トラフィックを 209.165.201.30 などの別のアドレスにリダイレクトします。

（注） **alias** コマンドを他のアドレスの変換ではなく DNS の書き換えに使用する場合は、エイリアス対応インターフェイスで **proxy-arp** をディセーブルにします。セキュリティ アプライアンスが一般的な NAT 処理のために **proxy-arp** でトラフィックを自身に引き寄せないようにするには、**sysopt noproxyarp** コマンドを使用します。

alias コマンドを変更または削除した後は、**clear xlate** コマンドを使用します。

DNS ゾーン ファイルに、**alias** コマンド内の「dnat」アドレスの A（アドレス）レコードが存在している必要があります。

alias コマンドには 2 つの使用方法があります。次にその概略を示します。

- セキュリティ アプライアンスが *mapped_ip* 宛てのパケットを取得した場合は、そのパケットを *real_ip* に送信するように **alias** コマンドを設定できます。
- セキュリティ アプライアンスがセキュリティ アプライアンスに戻された *real_ip* 宛ての DNS パケットを取得した場合は、DNS パケットを変更して、宛先ネットワーク アドレスを *mapped_ip* に変更するように **alias** コマンドを設定できます。

alias コマンドは、自動的にネットワーク上の DNS サーバと通信して、エイリアスが設定された IP アドレスへのドメイン名によるアクセスを透過的に処理します。

real_ip IP アドレスと *mapped_ip* IP アドレスにネットワーク アドレスを使用して、ネット エイリアスを指定します。たとえば、**alias 192.168.201.0 209.165.201.0 255.255.255.224** コマンドを実行すると、209.165.201.1 ～ 209.165.201.30 の各 IP アドレスのエイリアスが作成されます。

static コマンドと **access-list** コマンドで **alias** *mapped_ip* アドレスにアクセスするには、**access-list** コマンドで、許可されるトラフィックの発信元アドレスとして *mapped_ip* アドレスを指定します。次に例を示します。

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1 eq
ftp-data
hostname(config)# access-group acl_out in interface outside
```

内部アドレス 192.168.201.1 を宛先アドレス 209.165.201.1 にマッピングして、エイリアスを指定しています。

内部ネットワーク クライアント 209.165.201.2 が example.com に接続すると、内部クライアントのクエリーに対する外部 DNS サーバからの DNS 応答がセキュリティ アプライアンスによって 192.168.201.29 に変更されます。セキュリティ アプライアンスがグローバル プール IP アドレスとして 209.165.200.225 ～ 209.165.200.254 を使用する場合、パケットは SRC=209.165.201.2 および DST=192.168.201.29 でセキュリティ アプライアンスに送信されます。セキュリティ アプライアンスは、アドレスを外部の SRC=209.165.200.254 と DST=209.165.201.29 に変換します。

例

次に、内部ネットワークに IP アドレス 209.165.201.29 が含まれている例を示します。このアドレスはインターネット上にあり、example.com に属しています。内部クライアントが example.com にアクセスしようとしても、209.165.201.29 はローカルの内部ネットワーク上にあると見なされるため、パケットはセキュリティ アプライアンスに送信されません。この動作を修正するには、**alias** コマンドを次のように使用します。

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

次に、内部の 10.1.1.11 にある Web サーバと 209.165.201.11 で作成された **static** コマンドの例を示します。ソース ホストは外部にあり、アドレスは 209.165.201.7 です。外部の DNS サーバには、次に示すように www.example.com のレコードがあります。

```
dns-server# www.example.com. IN A 209.165.201.11
```

ドメイン名 www.example.com. の末尾のピリオドは 必要です。

次に、**alias** コマンドの使用例を示します。

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

セキュリティ アプライアンス は、内部クライアント用のネームサーバ応答を 10.1.1.11 に変更して、Web サーバに直接接続できるようにします。

アクセスを可能にするには、次のコマンドも必要です。

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq
telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストを作成します。
clear configure alias	すべての **alias** コマンドをコンフィギュレーションから削除します。
show running-config alias	コンフィギュレーション内のデュアル NAT コマンドと重複しているアドレスを表示します。
static	ローカル IP アドレスをグローバル IP アドレスに、またはローカル ポートをグローバル ポートにマッピングすることによって、1 対 1 のアドレス変換ルールを設定します。

allocate-interface

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るには、コンテキスト コンフィギュレーション モードで **allocate-interface** コマンドを使用します。インターフェイスをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]

no allocate-interface *physical_interface*

allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*]

構文の説明

invisible	（デフォルト）コンテキスト ユーザが **show interface** コマンドでマッピング名（設定されている場合）だけを表示できるようにします。

map_name	（任意）マッピング名を設定します。
	
	map_name は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス ID がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているインターフェイスをコンテキスト管理者に知らせない場合があります。
	
	マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。
	
	`int0`
	
	`inta`
	
	`int_0`
	
	サブインターフェイスの場合は、マッピング名の範囲を指定できます。
	
	範囲の詳細については、「使用上のガイドライン」を参照してください。

physical_interface	**gigabitethernet0/1** などのインターフェイス ID を設定します。有効値については、**interface** コマンドを参照してください。インターフェイス タイプとポート番号の間にスペースを含めないでください。
subinterface	サブインターフェイス番号を設定します。サブインターフェイスの範囲を指定できます。
visible	（任意）マッピング名を設定した場合でも、コンテキスト ユーザが **show interface** コマンドで物理インターフェイスのプロパティを表示できるようにします。

デフォルト

マッピング名を設定した場合、デフォルトでは、**show interface** コマンドの出力にインターフェイス ID は表示されません。

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	透過	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	•	•	—	—	•

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　このコマンドを複数回入力して、異なる範囲を指定できます。マッピング名または表示設定を変更するには、特定のインターフェイス ID に対してコマンドを再入力し、新しい値を設定します。**no allocate-interface** コマンドを入力して最初からやり直す必要はありません。**allocate-interface** コマンドを削除すると、セキュリティ アプライアンスによって、コンテキスト内のインターフェイス関連のコンフィギュレーションがすべて削除されます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

（注）　トランスペアレント モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをインターフェイスにフラッディングしません。

ルーテッド モードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレント モードでは、インターフェイスを共有できません。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。

  ```
  int0-int10
  ```

  たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力した場合、コマンドは失敗します。

- マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力した場合、コマンドは失敗します。

例

次に、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる例を示します。マッピング名は、int1 ～ int8 です。

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

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。
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 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 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。
vlan	サブインターフェイスに VLAN ID を割り当てます。

allocate-ips

IPS 仮想センサーをセキュリティ コンテキストに割り当てるには、AIP SSM がインストールされている場合には、コンテキスト コンフィギュレーション モードで **allocate-ips** コマンドを使用します。仮想センサーをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

構文の説明

default	（任意）コンテキストごとに 1 つのセンサーをデフォルト センサーとして設定します。コンテキスト コンフィギュレーションでセンサー名が指定されていない場合は、コンテキストでこのデフォルト センサーが使用されます。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。デフォルト センサーを変更する場合は、**no allocate-ips** *sensor_name* コマンドを入力して現在のデフォルト センサーを削除してから、新しいデフォルト センサーを割り当てます。センサーをデフォルトとして指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは AIP SSM のデフォルト センサーを使用します。
mapped_name	（任意）コンテキスト内で実際のセンサー名の代わりに使用できるセンサー名のエイリアスとして、マッピング名を設定します。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」および「sensor2」というセンサーを使用する場合、コンテキスト A の sensor1 と sensor2 に「highsec」センサーと「lowsec」センサーをマッピングし、コンテキスト B の sensor1 と sensor2 に「medsec」センサーと「lowsec」センサーをマッピングできます。
sensor_name	AIP SSM に設定されているセンサー名を設定します。AIP SSM に設定されているセンサーを表示するには、**allocate-ips ?** と入力します。使用可能なすべてのセンサーが表示されます。**show ips** コマンドを入力することもできます。システム実行スペースで **show ips** コマンドを入力すると、使用可能なすべてのセンサーが表示されます。このコマンドをコンテキストで入力すると、そのコンテキストにすでに割り当てられているセンサーが表示されます。AIP SSM にまだ存在しないセンサー名を指定した場合は、エラーが表示されますが、**allocate-ips** コマンドはそのまま入力されます。AIP SSM にその名前のセンサーが作成されるまで、コンテキストはそのセンサーがダウンしていると見なします。

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	透過	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	•	•	—	—	•

コマンド履歴

リリース	変更内容
8.0(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　各コンテキストに 1 つ以上の IPS 仮想センサーを割り当てることができます。その後、**ips** コマンドを使用して AIP SSM にトラフィックを送信するようにコンテキストを設定するときに、コンテキストに割り当てられているセンサーを指定できます。コンテキストに割り当てられていないセンサーは指定できません。コンテキストにセンサーが割り当てられていない場合は、AIP SSM に設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

（注）　仮想センサーを使用するためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

例　次に、sensor1 と sensor2 をコンテキスト A に、sensor1 と sensor3 をコンテキスト B に割り当てる例を示します。両方のコンテキストで、センサー名を「ips1」と「ips2」にマッピングします。コンテキスト A では sensor1 をデフォルト センサーとして設定しますが、コンテキスト B ではデフォルトを設定しないため、AIP SSM に設定されているデフォルトが使用されます。

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

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。
ips	トラフィックをインスペクションのために AIP SSM に転送します。
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 ips	AIP SSM に設定されている仮想センサーを表示します。

apcf

Application Profile Customization Framework プロファイルをイネーブルにするには、webvpn コンフィギュレーション モードで **apcf** コマンドを使用します。特定の APCF スクリプ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。すべての APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

apcf URL/filename.ext

no apcf [URL/filename.ext]

構文の説明

filename.extension	APCF カスタマイゼーション スクリプトの名前を指定します。これらのスクリプトは、常に XML 形式です。拡張子は、.xml、.txt、.doc などです。
URL	セキュリティ アプライアンスでロードして使用する APCF プロファイルの場所を指定します。http://、https://、tftp://、ftp://、flash:/、disk#:/' のいずれかの URL を使用します。 URL には、サーバ、ポート、およびパスを含めることができます。ファイル名のみを指定した場合、デフォルトの URL は flash:/ です。**copy** コマンドを使用して、APCF プロファイルをフラッシュ メモリにコピーできます。

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

次の表は、このコマンドを入力す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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

apcf コマンドを使用すると、セキュリティ アプライアンスは、非標準の Web アプリケーションと Web リソースを WebVPN 接続で正しくレンダリングされるように処理できます。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、どのデータを変換するかを指定するスクリプトがあります。

セキュリティ アプライアンスで複数の APCF プロファイルを使用できます。その場合、セキュリティ アプライアンスは、それらのプロファイルを古いものから新しいものの順に 1 つずつ適用します。

apcf コマンドは、Cisco TAC のサポートがある場合にのみ使用することを推奨します。

例

次に、フラッシュ メモリの /apcf にある apcf1 という名前の APCF をイネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

次に、myserver という名前の https サーバ（ポート 1440）のパス /apcf にある apcf2.xml という名前の APCF をイネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。
rewrite	トラフィックがセキュリティ アプライアンスを通過するかどうかを決定します。
show running config webvpn apcf	APCF 設定を表示します。

appl-acl

セッションに適用する設定済みの Web タイプ ACL を指定するには、DAP webvpn コンフィギュレーション モードで **appl-acl** 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するには、このコマンドの **no** 形式を使用します。すべての Web タイプ ACL を削除するには、このコマンドの **no** 形式を引数なしで使用します。

appl-acl *identifier*

no appl-acl [*identifier***]**

構文の説明

identifier	設定済みの Web タイプ ACL の名前（最大 240 文字）。

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	透過	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

Web タイプ ACL 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 **access-list_webtype** コマンドを使用します。

appl-acl コマンドを複数回使用して、複数の Web タイプ ACL を DAP ポリシーに適用できます。

例

次に、newacl という名前の設定済みの Web タイプ ACL をダイナミック アクセス ポリシーに適用する例を示します。

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dynamic-access-policy-record)# appl-acl newacl
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
access-list_webtype	Web タイプ ACL を作成します。

application-access

認証された WebVPN ユーザに表示される WebVPN ホームページの [Application Access] フィールド、およびユーザがアプリケーションを選択したときに表示される [Application Access] ウィンドウをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **application-access** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

no application-access {**title** | **message** | **window**} {**text** | **style**} *value*

構文の説明

message	[Application Access] フィールドのタイトルの下に表示されるメッセージを変更します。
style	[Application Access] フィールドのスタイルを変更します。
text	[Application Access] フィールドのテキストを変更します。
title	[Application Access] フィールドのタイトルを変更します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。
window	[Application Access] ウィンドウを変更します。

デフォルト

[Application Access] フィールドのデフォルトのタイトル テキストは「Application Access」です。

[Application Access] フィールドのデフォルトのタイトル スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

[Application Access] フィールドのデフォルトのメッセージ テキストは「Start Application Client」です。

[Application Access] フィールドのデフォルトのメッセージ スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller.

[Application Access] ウィンドウのデフォルトのウィンドウ テキストは次のとおりです。

「Close this window when you finish using Application Access.Please wait for the table to be displayed before starting applications.」

[Application Access] ウィンドウのデフォルトのウィンドウ スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

このコマンドには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

次に、WebVPN ページに対する変更で最もよく行われるページ配色の変更に役立つヒントを紹介します。

- 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。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Application Access] フィールドの背景色を RGB 16 進値 66FFFF（緑色の一種）にカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

関連コマンド

コマンド	説明
application-access hide-details	[Application Access] ウィンドウのアプリケーション詳細の表示をイネーブルまたはディセーブルにします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

application-access hide-details

WebVPN の [Application Access] ウィンドウに表示されるアプリケーション詳細を非表示にするには、カスタマイゼーション コンフィギュレーション モードで **application-access hide-details** コマンドを使用します。このモードには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access hide-details {**enable | disable**}

no application-access [**hide-details** {**enable | disable**}]

構文の説明

disable	[Application Access] ウィンドウにアプリケーション詳細を表示します。
enable	[Application Access] ウィンドウのアプリケーション詳細を非表示にします。

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。[Application Access] ウィンドウにアプリケーション詳細が表示されます。

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	透過	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、アプリケーション詳細の表示をディセーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# application-access hide-details disable
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] フィールドをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。

area

OSPF エリアを作成するには、ルータ コンフィギュレーション モードで **area** コマンドを使用します。エリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id*

no area *area_id*

構文の説明

area_id	作成するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

作成したエリアには、パラメータが設定されていません。関連する area コマンドを使用してエリア パラメータを設定します。

例

次に、エリア ID が 1 の OSPF エリアを作成する例を示します。

```
hostname(config-router)# area 1
hostname(config-router)#
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
area stub	エリアをスタブ エリアとして定義します。
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area authentication

OSPF エリアの認証をイネーブルにするには、ルータ コンフィギュレーション モードで **area authentication** コマンドを使用します。

エリア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。

area *area_id* **authentication** [**message-digest**]

no area *area_id* **authentication** [**message-digest**]

構文の説明

area_id	認証をイネーブルにするエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
message-digest	（任意）*area_id* で指定したエリアに対する Message Digest 5（MD5）認証をイネーブルにします。

デフォルト

エリア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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定した OSPF エリアが存在しない場合は、このコマンドを入力すると作成されます。**message-digest** キーワードを指定せずに **area authentication** コマンドを入力した場合は、簡易パスワード認証がイネーブルになります。**message-digest** キーワードを指定すると、MD5 認証がイネーブルになります。

例

次に、エリア 1 に対して MD5 認証をイネーブルにする例を示します。

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

関連コマンド

コマンド	説明
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area default-cost

スタブまたは NSSA に送信されるデフォルト集約ルートのコストを指定するには、ルータ コンフィギュレーション モードで **area default-cost** コマンドを使用します。デフォルトのコスト値に戻すには、このコマンドの **no** 形式を使用します。

area *area_id* **default-cost** *cost*

no area *area_id* **default-cost**

構文の説明

area_id	デフォルト コストを変更するスタブまたは NSSA の ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
cost	スタブまたは NSSA に使用されるデフォルト集約ルートのコストを指定します。有効な値の範囲は、0 ～ 65535 です。

デフォルト

cost のデフォルト値は 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

例

次に、スタブまたは NSSA に送信される集約ルートのデフォルト コストを指定する例を示します。

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
area stub	エリアをスタブ エリアとして定義します。

コマンド	説明
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area filter-list prefix

ABR の OSPF エリア間のタイプ 3 LSA でアドバタイズされたプレフィックスをフィルタリングするには、ルータ コンフィギュレーション モードで **area filter-list prefix** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの **no** 形式を使用します。

area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

no area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

構文の説明

area_id	フィルタリングを設定するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
in	指定したエリアに着信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。
list_name	プレフィックス リストの名前を指定します。
out	指定したエリアから発信されるアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

フィルタリングできるのはタイプ 3 LSA だけです。プライベート ネットワークに ASBR が設定されている場合、ASBR はプライベート ネットワークを記述するタイプ 5 LSA を送信します。この LSA は、パブリック エリアを含む AS 全体にフラッディングされます。

例

次に、他のすべてのエリアからエリア 1 に送信されるプレフィックスをフィルタリングする例を示します。

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

関連コマンド

コマンド	説明
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area nssa

エリアを NSSA として設定するには、ルータ コンフィギュレーション モードで **area nssa** コマンドを使用します。NSSA 指定をエリアから削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

構文の説明

area_id	NSSA として指定するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
default-information-originate	NSSA エリアでのタイプ 7 デフォルトの生成に使用します。このキーワードは、NSSA ABR または NSSA ASBR でのみ有効です。
metric *metric_value*	（任意）OSPF デフォルト メトリック値を指定します。有効値の範囲は 0 ～ 16777214 です。
metric-type {**1** | **2**}	（任意）デフォルト ルートの OSPF メトリック タイプ。有効な値は次のとおりです。 • **1**：タイプ 1 • **2**：タイプ 2 デフォルト値は 2 です。
no-redistribution	（任意）ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA エリアでなく通常のエリアにのみ取り込む場合に使用します。
no-summary	（任意）エリアを Not-So-Stubby Area（NSSA）とし、集約ルートが挿入されないようにします。

デフォルト

デフォルトの設定は次のとおりです。

- NSSA エリアは未定義です。
- **metric-type** は 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

エリアに 1 つのオプションを設定し、後で別のオプションを指定した場合、両方のオプションが設定されます。たとえば、次の 2 のコマンドを別々に入力した場合、コンフィギュレーションには、両方のオプションを指定した 1 つのコマンドが設定されます。

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

例

次に、2 つのオプションを別々に設定すると、1 つのコマンドがコンフィギュレーションに設定される例を示します。

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

関連コマンド

コマンド	説明
area stub	エリアをスタブ エリアとして定義します。
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area range

エリア境界でルートを統合および集約するには、ルータ コンフィギュレーション モードで **area range** 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。

area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

no area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

構文の説明

address	サブネット範囲の IP アドレス。
advertise	（任意）Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。
area_id	範囲を設定するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
mask	IP アドレスのサブネット マスク。
not-advertise	（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。

デフォルト

アドレス範囲ステータスは advertise 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

area range コマンドは、ABR でのみ使用されます。このコマンドによって、エリアのルートが統合または集約されます。その結果、1 つの集約ルートが ABR によって他のエリアにアドバタイズされます。ルーティング情報は、エリア境界でまとめられます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作は*ルート集約*と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。したがって、OSPF は、多くの異なるアドレス範囲セットのアドレスを集約できます。

no area *area_id* **range** *ip_address netmask* **not-advertise** コマンドは、**not-advertise** オプション キーワードのみを削除します。

例

次に、ネットワーク 10.0.0.0 上のすべてのサブネットおよびネットワーク 192.168.110.0 上のすべてのホストに対する 1 つの集約ルートを、ABR によって他のエリアにアドバタイズするように指定する例を示します。

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area stub

エリアをスタブ エリアとして定義するには、ルータ コンフィギュレーション モードで **area stub** コマンドを使用します。スタブ エリア機能を削除するには、このコマンドの **no** 形式を使用します。

area *area_id* [**no-summary**]

no area *area_id* [**no-summary**]

構文の説明

area_id	スタブ エリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
no-summary	ABR がサマリー リンク アドバタイズメントをスタブ エリアに送信しないようにします。

デフォルト

デフォルトの動作は次のとおりです。

- スタブ エリアは定義されません。
- サマリー リンク アドバタイズメントはスタブ エリアに送信されます。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、スタブまたは NSSA に接続された ABR でのみ使用されます。

スタブ エリア ルータ コンフィギュレーション コマンドには、**area stub** および **area default-cost** という 2 つのコマンドがあります。スタブ エリアに接続されているすべてのルータおよびアクセス サーバで、**area stub** コマンドを使用して、エリアをスタブ エリアとして設定する必要があります。スタブ エリアに接続された ABR でのみ **area default-cost** コマンドを使用します。**area default-cost** コマンドは、ABR によって生成される集約デフォルト ルートのメトリックをスタブ エリアに提供します。

例

次に、指定したエリアをスタブ エリアとして設定する例を示します。

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

関連コマンド

コマンド	説明
area default-cost	スタブまたは NSSA に送信されるデフォルト集約ルートのコストを指定します。
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area virtual-link

OSPF 仮想リンクを定義するには、ルータ コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットするか、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

no area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

構文の説明

area_id	仮想リンクの中継エリアのエリア ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
authentication	（任意）認証タイプを指定します。
authentication-key *key*	（任意）ネイバー ルーティング デバイスで使用する OSPF 認証パスワードを指定します。
dead-interval *seconds*	（任意）hello パケットを受信しない場合に、ネイバー ルーティング デバイスがダウンしたことを宣言するまでの間隔を指定します。有効な値は、1 ～ 65535 秒です。
hello-interval *seconds*	（任意）インターフェイスで送信される hello パケット間の間隔を指定します。有効な値は、1 ～ 65535 秒です。
md5 *key*	（任意）最大 16 バイトの英数字のキーを指定します。
message-digest	（任意）メッセージ ダイジェスト認証を使用することを指定します。
message-digest-key *key_id*	（任意）Message Digest 5（MD5）認証をイネーブルにし、認証キー ID 番号を指定します。有効な値は、1 ～ 255 です。
null	（任意）認証を使用しないことを指定します。パスワードまたはメッセージ ダイジェスト認証は、OSPF エリアに設定されている場合、上書きされます。
retransmit-interval *seconds*	（任意）インターフェイスに属している隣接ルータの LSA 再送信の間隔を指定します。有効な値は、1 ～ 65535 秒です。
router_id	仮想リンク ネイバーに関連付けられているルータ ID。ルータ ID は、各ルータによって内部でインターフェイス IP アドレスから生成されます。この値は、IP アドレスの形式で入力する必要があります。デフォルトはありません。
transmit-delay *seconds*	（任意）OSPF がトポロジ変更を受信してから、Shortest Path First（SPF）計算を開始するまでの遅延時間を 0 ～ 65535 秒で指定します。デフォルトは 5 秒です。

デフォルト

デフォルトの設定は次のとおりです。

- *area_id*：エリア ID は事前に定義されていません。
- *router_id*：ルータ ID は事前に定義されていません。
- **hello-interval** *seconds*：10 秒。
- **retransmit-interval** *seconds*：5 秒。

- **transmit-delay** *seconds*：1 秒。
- **dead-interval** *seconds*：40 秒。
- **authentication-key** *key*：キーは事前に定義されていません。
- **message-digest-key** *key_id* **md5** *key*：キーは事前に定義されていません。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。

hello 間隔を小さくすればするほど、トポロジ変更の検出が速くなりますが、ルーティング トラフィックが増加します。

再送信間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

指定した認証キーは、**area** *area_id* **authentication** コマンドでバックボーンに対して認証がイネーブルにされている場合にのみ使用されます。

簡易テキスト認証と MD5 認証という 2 つの認証方式は、相互排他的です。どちらか一方を指定するか、または両方とも指定しないでください。**authentication-key** *key* または **message-digest-key** *key_id* **md5** *key* の後に指定したキーワードと引数は、すべて無視されます。したがって、オプションの引数は、これらのキーワードと引数の組み合わせの前に指定します。

インターフェイスに認証タイプが指定されていない場合、インターフェイスでは、エリアに指定されている認証タイプが使用されます。エリアに認証タイプが指定されていない場合、エリアのデフォルトはヌル認証です。

（注） 仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク隣接ルータ ID が含まれている必要があります。ルータ ID を表示するには、**show ospf** コマンドを使用します。

仮想リンクからオプションを削除するには、削除するオプションを指定して、このコマンドの **no** 形式を使用します。仮想リンクを削除するには、**no area** *area_id* **virtual-link** コマンドを使用します。

例

次に、MD5 認証の仮想リンクを確立する例を示します。

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
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	OSPF ルーティング プロセスに関する一般情報を表示します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

arp

スタティック ARP エントリを ARP テーブルに追加するには、グローバル コンフィギュレーション モードで **arp** コマンドを使用します。スタティック 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。スタティック ARP エントリは、MAC アドレスを IP アドレスにマッピングし、ホストに到達するまでに通過するインターフェイスを指定します。スタティック ARP エントリはタイムアウトせず、ネットワーク問題の解決に役立つ場合があります。トランスペアレント ファイアウォール モードでは、ARP インスペクションでスタティック ARP テーブルが使用されます（**arp-inspection** コマンドを参照）。

arp *interface_name ip_address mac_address* [**alias**]

no arp *interface_name ip_address mac_address*

構文の説明

alias	（任意）このマッピングに対してプロキシ ARP をイネーブルにします。セキュリティ アプライアンスは、指定された IP アドレスに対する ARP 要求を受信すると、セキュリティ アプライアンスの MAC アドレスで応答します。その IP アドレスを持つホスト宛てのトラフィックをセキュリティ アプライアンスが受信すると、セキュリティ アプライアンスは、トラフィックをこのコマンドで指定されたホスト MAC アドレスに転送します。このキーワードは、ARP を実行しないデバイスがある場合などに役立ちます。 トランスペアレント ファイアウォール モードでは、このキーワードは無視され、セキュリティ アプライアンスでプロキシ ARP は実行されません。
interface_name	ホスト ネットワークに接続されているインターフェイス。
ip_address	ホストの IP アドレス。
mac_address	ホストの MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ホストは IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求

を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、エントリは更新される前にタイムアウトします。

（注）　トランスペアレント ファイアウォール モードでは、ダイナミック ARP エントリがセキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）に使用されます。

例

次に、外部インターフェイス上の 10.1.1.1 と MAC アドレス 0009.7cbe.2100 のスタティック ARP エントリを作成する例を示します。

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

関連コマンド

コマンド	説明
arp timeout	セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
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 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。

arp timeout

セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定するには、グローバル コンフィギュレーション モードで **arp timeout** コマンドを使用します デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。ARP テーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

arp timeout *seconds*

no arp timeout *seconds*

構文の説明

seconds	ARP テーブルを再構築する間隔の秒数（60 ～ 4294967）。

デフォルト

デフォルト値は 14,400 秒（4 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、ARP タイムアウトを 5,000 秒に変更する例を示します。

```
hostname(config)# arp timeout 5000
```

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	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp timeout	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。

arp-inspection

トランスペアレント ファイアウォール モードでの ARP インスペクショ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 **arp-inspection** コマンドを使用します。ARP インスペクショ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。ARP インスペクションでは、すべての ARP パケットをスタティック ARP エントリと照合し（**arp** コマンドを参照）、一致しないパケットをブロックします。この機能により、ARP スプーフィングが防止されます。

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

no arp-inspection *interface_name* **enable**

構文の説明

enable	ARP インスペクションをイネーブルにします。
flood	（デフォルト）スタティック ARP エントリのどの要素とも一致しないパケットをすべてのインターフェイス（発信元インターフェイスを除く）にフラッディングすることを指定します。MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、セキュリティ アプライアンスはパケットをドロップします。 **（注）** 管理専用のインターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。
interface_name	ARP インスペクションをイネーブルにするインターフェイス。
no-flood	（任意）スタティック ARP エントリと正確には一致しないパケットをドロップすることを指定します。

デフォルト

デフォルトでは、ARP インスペクションはすべてのインターフェイスでディセーブルになっています。すべての ARP パケットはセキュリティ アプライアンスを通過できます。ARP インスペクションをイネーブルにすると、一致しない ARP パケットはデフォルトでフラッディングされます。

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	透過	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	—	•	•	•	—

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

ARP インスペクションをイネーブルにする前に、**arp** コマンドを使用してスタティック ARP エントリを設定します。

ARP インスペクションをイネーブルにすると、セキュリティ アプライアンスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、セキュリティ アプライアンスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにセキュリティ アプライアンスを設定できます。

（注） 専用の管理インターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

ARP インスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホスト トラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

（注） トランスペアレント ファイアウォール モードでは、ダイナミック ARP エントリがセキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）に使用されます。

例

次に、外部インターフェイスにおける ARP インスペクションをイネーブルにし、スタティック ARP エントリに一致しない ARP パケットをドロップするようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

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。
clear configure arp-inspection	ARP インスペクション コンフィギュレーションをクリアします。
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。
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。

asdm disconnect

アクティブな ASDM セッションを終了するには、特権 EXEC モードで **asdm disconnect** コマンドを使用します。

asdm disconnect *session*

構文の説明

session	終了するアクティブな ASDM セッションのセッション ID。**show asdm sessions** コマンドを使用して、すべてのアクティブな ASDM セッションのセッション ID を表示できます。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm disconnect** コマンドが **asdm disconnect** 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 ASDM セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm sessions** コマンドを使用します。特定のセッションを終了するには、**asdm disconnect** コマンドを使用します。

ASDM セッションを終了しても、残りのアクティブな ASDM セッションは、関連付けられているセッション ID を保持します。たとえば、3 つのアクティブな ASDM セッションがあり、それぞれのセッション ID が 0、1、および 2 の場合、セッション 1 を終了すると、残りのアクティブな ASDM セッションはそれぞれセッション ID 0 と 2 を保持します。この例で、次の新しい ASDM セッションにはセッション ID 1 が割り当てられ、その後の新しいセッションにはセッション ID 3 から順に ID が割り当てられます。

例

次に、セッション ID 0 の ASDM セッションを終了する例を示します。**asdm disconnect** コマンドの入力の前後に、**show asdm sessions** コマンドを使用して、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions
```

```
1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm sessions	アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm disconnect log_session

アクティブな ASDM ロギング セッションを終了するには、特権 EXEC モードで **asdm disconnect log_session** コマンドを使用します。

asdm disconnect log_session *session*

構文の説明

session	終了するアクティブな ASDM ロギング セッションのセッション ID。**show asdm log_sessions** コマンドを使用して、すべてのアクティブな ASDM セッションのセッション ID を表示できます。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

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

アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm log_sessions** コマンドを使用します。特定のロギング セッションを終了するには、**asdm disconnect log_session** コマンドを使用します。

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、セキュリティ アプライアンスから Syslog メッセージを取得します。ログ セッションを終了すると、アクティブな ASDM セッションに悪影響が及ぶ場合があります。不要な ASDM セッションを終了するには、**asdm disconnect** コマンドを使用します。

（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。

ASDM ロギング セッションを終了しても、残りのアクティブな ASDM ロギング セッションは、関連付けられているセッション ID を保持します。たとえば、3 つのアクティブな ASDM ロギング セッションがあり、それぞれのセッション ID が 0、1、および 2 の場合、セッション 1 を終了すると、残りのアクティブな ASDM ロギング セッションはそれぞれセッション ID 0 と 2 を保持します。この例で、次の新しい ASDM ロギング セッションにはセッション ID 1 が割り当てられ、その後の新しいロギング セッションにはセッション ID 3 から順に ID が割り当てられます。

例

次に、セッション ID 0 の ASDM セッションを終了する例を示します。**asdm disconnect log_sessions** コマンドの入力の前後に、**show asdm log_sessions** コマンドを使用して、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm log_sessions	アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm history enable

ASDM 履歴トラッキング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 **asdm history enable** コマンドを使用します。ASDM 履歴トラッキ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。

asdm history enable

no asdm history 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	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**pdm history enable** コマンドが **asdm history enable** コマンドに変更されました。

使用上のガイドライン

ASDM 履歴トラッキングをイネーブルにすることによって取得された情報は、ASDM 履歴バッファに保存されます。この情報は、**show asdm history** コマンドを使用して表示できます。履歴情報は、ASDM によってデバイス モニタリングに使用されます。

例

次に、ASDM 履歴トラッキングをイネーブルにする例を示します。

```
hostname(config)# asdm history enable
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

asdm image

フラッシュ メモリ内の ASDM ソフトウェア イメージの場所を指定するには、グローバル コンフィギュレーション モードで **asdm image** コマンドを使用します。イメージの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。

asdm image *url*

no asdm image [*url*]

構文の説明

url	フラッシュ メモリ内の ASDM イメージの場所を設定します。次の URL 構文を参照してください。 • **disk0:**/[*path*/]*filename* ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内部フラッシュ メモリを指します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:**/[*path*/]*filename* ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。 • **flash:**/[*path*/]*filename* この URL は内部フラッシュ メモリを示します。

デフォルト

このコマンドをスタートアップ コンフィギュレーションに含めない場合、セキュリティ アプライアンスは起動時に最初に検出した ASDM イメージを使用します。内部フラッシュ メモリのルート ディレクトリ内を検索した後で、外部フラッシュ メモリを検索します。セキュリティ アプライアンスはイメージを検出した場合は、**asdm image** コマンドを実行コンフィギュレーションに挿入します。

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	透過	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	•	•	•	—	•

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

フラッシュ メモリに複数の ASDM ソフトウェア イメージを保存できます。アクティブな ASDM セッションがある状態で **asdm image** コマンドを入力して新しい ASDM ソフトウェア イメージを指定した場合、アクティブな ASDM セッションは中断されず、そのセッションを開始した ASDM ソフトウェア イメージを引き続き使用します。新しい ASDM セッションは、新しいソフトウェア イメージを使用

します。**no asdm image** コマンドを入力すると、コンフィギュレーションからコマンドが削除されます。ただし、最後に設定したイメージの場所を使用して、セキュリティ アプライアンスから引き続き ASDM にアクセスできます。

このコマンドをスタートアップ コンフィギュレーションに含めない場合、セキュリティ アプライアンスは起動時に最初に検出した ASDM イメージを使用します。内部フラッシュ メモリのルート ディレクトリ内を検索した後で、外部フラッシュ メモリを検索します。セキュリティ アプライアンスはイメージを検出した場合は、**asdm image** コマンドを実行コンフィギュレーションに挿入します。**write memory** コマンドを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存してください。**asdm image** コマンドをスタートアップ コンフィギュレーションに保存しない場合、リブートのたびにセキュリティ アプライアンスは ASDM イメージを検索し、**asdm image** コマンドを実行コンフィギュレーションに挿入します。Auto Update を使用する場合は、起動時にこのコマンドが自動的に追加されるため、セキュリティ アプライアンス上のコンフィギュレーションは Auto Update Server 上のコンフィギュレーションと一致しなくなります。このような不一致が発生すると、セキュリティ アプライアンスはコンフィギュレーションを Auto Update Server からダウンロードします。不要な Auto Update アクティビティを回避するには、**asdm image** コマンドをスタートアップ コンフィギュレーションに保存します。

例

次に、ASDM イメージを asdm.bin に設定する例を示します。

```
hostname(config)# asdm image flash:/asdm.bin
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm image	現在の ASDM イメージ ファイルを表示します。
boot	ソフトウェア イメージとスタートアップ コンフィギュレーション ファイルを設定します。

asdm location

注意　このコマンドを手動で設定しないでください。**asdm location** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部通信に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

構文の説明

ip_addr	ネットワーク トポロジを定義するために ASDM によって内部で使用される IP アドレス。
netmask	*ip_addr* のサブネット マスク。
if_name	ASDM にアクセスするときに通過するインターフェイスの名前。
ipv6_addr/prefix	ネットワーク トポロジを定義するために ASDM によって内部で使用される IPv6 アドレスとプレフィックス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm location** コマンドが **asdm location** コマンドに変更されました。

使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

asr-group

非対称ルーティング インターフェイス グループ 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 **asr-group** 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。

asr-group *group_id*

no asr-group *group_id*

構文の説明

group_id	非対称ルーティング グループ ID。有効な値は、1 ～ 32 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	透過	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	•	•	—	•	—

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

Active/Active フェールオーバーがイネーブルの場合、ロード バランシングにより、発信接続のリターン トラフィックがピア ユニット上のアクティブなコンテキストを介してルーティングされることがあります。このピア ユニットでは、発信接続のコンテキストはスタンバイ グループ内にあります。

asr-group コマンドを使用すると、着信インターフェイスのフローが見つからない場合に、着信パケットが同じ asr-group のインターフェイスで再分類されます。再分類により別のインターフェイスのフローが見つかり、関連付けられているコンテキストがスタンバイ状態の場合、パケットは処理のためにアクティブなユニットに転送されます。

このコマンドを有効にするには、ステートフル フェールオーバーをイネーブルにする必要があります。

ASR 統計情報は、**show interface detail** コマンドを使用して表示できます。この統計情報には、インターフェイス上で送信、受信、およびドロップされた ASR パケットの数が含まれます。

例

次に、選択したインターフェイスを非対称ルーティング グループ 1 に割り当てる例を示します。

コンテキスト ctx1 のコンフィギュレーション：

```
hostname/ctx1(config)# interface Ethernet2
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

コンテキスト ctx2 のコンフィギュレーション：

```
hostname/ctx2(config)# interface Ethernet3
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

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 interface	インターフェイス統計情報を表示します。

assertion-consumer-url

セキュリティ デバイスがアサーション コンシューマ サービスに接続するためにアクセスする URL を指定するには、webvpn コンフィギュレーション モードで、特定の SAML-type SSO サーバに対して **assertion-consumer-url** コマンドを使用します。

この URL をアサ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。

assertion-consumer-url *url*

no assertion-consumer-url [*url*]

構文の説明

url	SAML-type SSO サーバで使用するアサーション コンシューマ サービスの URL を指定します。URL は http:// または https: で始まり、255 文字未満の英数字である必要があります。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

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。セキュリティ アプライアンスは現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

URL が HTTPS で始まる場合は、アサーション コンシューマ サービスの SSL 証明書のルート証明書をインストールする必要があります。

次に、SAML-type の SSO サーバのアサーション コンシューマ URL を指定する例を示します。

```
hostname(config-webvpn)# sso server myhostname type saml-v1.1-post
hostname(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
hostname(config-webvpn-sso-saml#
```

関連コマンド

コマンド	説明
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。
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	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	WebVPN シングル サインオン サーバを作成します。
trustpoint	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。

attribute

セキュリティ アプライアンスが DAP 属性データベースに書き込む属性値ペアを指定するには、DAP テスト属性モードで **attribute** コマンドを使用します。複数の属性値ペアを入力するには、このコマンドを複数回使用します。

attribute *name value*

構文の説明

name	既知の属性名、または「label」タグを組み込む属性を指定します。label タグは、DAP レコード内のファイル、レジストリ、プロセス、アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォールのエンドポイント属性に対して設定するエンドポイント ID に対応します。
value	AAA 属性に割り当てられた値。

コマンド 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	透過	シングル	コンテキスト	システム
DAP 属性コンフィギュレーション モード	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

通常、セキュリティ アプライアンスは AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。セキュリティ アプライアンスは、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。

例

次の例では、認証されたユーザが SAP グループのメンバーで、エンドポイント システムにアンチウイルス ソフトウェアがインストールされている場合に、セキュリティ アプライアンスが 2 つの DAP レコードを選択することを前提としています。アンチウイルス ソフトウェアのエンドポイント ルールのエンドポイント ID は *nav* です。

DAP レコードには、次のポリシー属性があります。

DAP レコード 1	DAP レコード 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2
	url-entry = enable

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)# attribute aaa.ldap.memberof SAP
hostname(config-dap-test-attr)# attribute endpoint.av.nav.exists true
hostname(config-dap-test-attr)# exit

hostname # test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable

hostname #
```

関連コマンド

コマンド	説明
display	現在の属性リストを表示します。
dynamic-access-policy-record	DAP レコードを作成します。
test dynamic-access-policy attributes	属性サブモードを開始します。
test dynamic-access-policy execute	DAP を生成するロジックを実行し、生成されたアクセス ポリシーをコンソールに表示します。

auth-cookie-name

認証クッキーの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **auth-cookie-name** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。

auth-cookie-name

構文の説明

name	認証クッキーの名前。名前の最大の長さは 128 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(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

セキュリティ アプライアンスの WebVPN サーバは、SSO サーバにシングル サインオン認証要求を送信することに HTTP POST 要求を使用します。認証が成功すると、認証 Web サーバは、認証クッキーをクライアント ブラウザに戻します。クライアント ブラウザは、その認証クッキーを提示して、SSO ドメイン内の他の Web サーバの認証を受けます。**auth-cookie-name** コマンドは、セキュリティ アプライアンスによって SSO に使用される認証クッキーの名前を設定します。

一般的な認証クッキーの形式は、Set-Cookie: <cookie name>=<cookie value> [;<cookie attributes>] です。次の認証クッキーの例では、SMSESSION が **auth-cookie-name** コマンドで設定される名前です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o8
8uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5d
c/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Pa
th=/
```

例

次に、example.com という名前の Web サーバから受信した認証クッキーに認証クッキー名 SMSESSION を指定する例を示します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# auth-cookie-name SMSESSION
hostname(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。
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。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	ユーザ名パラメータを SSO 認証に使用される HTTP POST 要求の一部として送信する必要があることを指定します。

authentication-certificate

接続を確立している WebVPN クライアントから証明書を要求するには、webvpn コンフィギュレーション モードで **authentication-certificate** コマンドを使用します。クライアント証明書の要求をキャンセルするには、このコマンドの **no** 形式を使用します。

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

構文の説明

interface-name	接続を確立するために使用するインターフェイスの名前。使用可能なインターフェイス名は、次のとおりです。 • **inside**　GigabitEthernet0/1 インターフェイスの名前 • **outside**　GigabitEthernet0/0 インターフェイスの名前

デフォルト

- **authentication-certificate** コマンドを省略すると、クライアント証明書認証はディセーブルになります。
- interface-name を **authentication-certificate** コマンドで指定しない場合、デフォルトの interface-name は **inside** 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

このコマンドを有効にするには、WebVPN が対応するインターフェイスですでに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設定して名前を付けるには、**interface**、**IP address**、および **nameif** コマンドを使用します。

このコマンドは、WebVPN クライアント接続にのみ適用されます。ただし、**管理**接続のクライアント証明書認証を **http authentication-certificate** コマンドを使って指定することは、WebVPN をサポートしないプラットフォームも含めてすべてのプラットフォームで可能です。

セキュリティ アプライアンスは、PKI トラストポイントに対して証明書を検証します。証明書が検証に合格しない場合、次のいずれかのアクションが実行されます。

条件	実行されるアクション
セキュリティ アプライアンスに組み込まれているローカル CA がイネーブルでない場合。	セキュリティ アプライアンスは SSL 接続を閉じます。
ローカル CA はイネーブルであるが、AAA 認証がイネーブルでない場合。	セキュリティ アプライアンスは証明書を取得するために、クライアントをローカル CA の証明書登録ページにリダイレクトします。
ローカル CA と AAA 認証の両方がイネーブルの場合。	クライアントは AAA 認証ページにリダイレクトされます。設定されている場合、ローカル CA の登録ページのリンクもクライアントに表示します。

例

次に、外部インターフェイスの WebVPN ユーザ接続の証明書認証を設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
authentication（トンネル グループ **webvpn** コンフィギュレーション モード）	トンネル グループのメンバーは認証にデジタル証明書を使用する必要があることを指定します。
http authentication-certificate	認証にセキュリティ アプライアンスへの ASDM 管理接続用の証明書を使用することを指定します。
interface	接続の確立に使用するインターフェイスを設定します。
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 trust-point	SSL 証明書トラストポイントを設定します。

authentication-exclude

エンド ユーザがクライアントレス SSL VPN にログインせずに設定済みリンクを参照できるようにするには、webvpn モードで **authentication-exclude** コマンドを使用します。複数のサイトへのアクセスを許可するには、このコマンドを複数回使用します。

authentication-exclude *url-fnmatch*

構文の説明

url-fnmatch	クライアントレス SSL VPN へのログインの要件を免除するリンクを指定します。

コマンド デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

この機能は、一部の内部リソースを SSL VPN 経由で一般利用できるようにする場合に便利です。

リンクに関する情報を、SSL VPN マングリングした形式でエンド ユーザに配布する必要があります。たとえば、SSL VPN を使用してこれらのリソースを参照し、配布するリンクに関する情報に結果の URL をコピーします。

例

次に、2 つのサイトに対して認証要件を免除する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-exclude http://www.site.com/public/*
hostname(config-webvpn)#authentication-exclude *announcement.html
hostname(config-webvpn)# hostname #
```

authentication

WebVPN と電子メール プロキシの認証方式を設定するには、各モードで **authentication** コマンドを使用します。デフォルトの方式に戻すには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、ユーザを認証してユーザ ID を確認します。

authentication {[**aaa**] [**certificate**] [**mailhost**] [**piggyback**]}

no authentication [**aaa**] [**certificate**] [**mailhost**] [**piggyback**]

構文の説明

aaa	セキュリティ アプライアンスが設定済みの AAA サーバと照合するユーザ名およびパスワードを指定します。
certificate	SSL ネゴシエーション時の証明書を指定します。
mailhost	リモート メール サーバを介して認証します。SMTPS の場合にのみ使用します。IMAP4S および POP3S の場合、メールホスト認証は必須であり、設定可能なオプションとして表示されません。
piggyback	HTTPS WebVPN セッションがすでに存在している必要があります。ピギーバック認証は、電子メール プロキシでのみ使用できます。

デフォルト

次の表に、WebVPN および電子メール プロキシのデフォルトの認証方式を示します。

プロトコル	デフォルトの認証方式
IMAP4S	メールホスト（必須）
POP3S	メールホスト（必須）
SMTPS	AAA
WebVPN	AAA

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、WebVPN 用のトンネル グループ webvpn 属性コンフィギュレーション モードに置き換えられました。
8.0(2)	このコマンドは、証明書認証要件の変更を反映するように変更されました。

使用上のガイドライン

少なくとも 1 つの認証方式が必要です。たとえば、WebVPN の場合、AAA 認証と証明書認証のいずれか一方または両方を指定できます。これらは、どちらを先に指定してもかまいません。

WebVPN 証明書認証では、それぞれのインターフェイスに対して HTTPS ユーザ証明書を要求する必要があります。つまり、この選択が機能するには、証明書認証を指定する前に、**authentication-certificate** コマンドでインターフェイスを指定しておく必要があります。

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn 属性コンフィギュレーション モードの同等のコマンドに変換されます。

WebVPN の場合、AAA 認証と証明書認証の両方を要求できます。その場合、ユーザは証明書およびユーザ名とパスワードを指定する必要があります。電子メール プロキシ認証の場合、複数の認証方式を要求できます。このコマンドを再び指定すると、現在のコンフィギュレーションが上書きされます。

例

次に、WebVPN ユーザに認証のための証明書を要求する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication certificate
```

関連コマンド

コマンド	説明
authentication-certificate	接続を確立する WebVPN クライアントからの証明書を要求します。
show running-config	現在のトンネル グループ コンフィギュレーションを表示します。
clear configure aaa	設定済みの AAA の値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

authentication eap-proxy

L2TP over IPSec 接続に対して EAP をイネーブルにし、セキュリティ アプライアンスが PPP 認証プロセスを外部の RADIUS 認証サーバにプロキシできるようにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication eap-proxy** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication eap-proxy

no authentication eap-proxy

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

デフォルトでは、EAP は認証プロトコルとして許可されていません。

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	透過	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

この属性は、L2TP/IPSec トンネル グループ タイプのみに適用できます。

例

次に、設定 ppp コンフィギュレーション モードで、pppremotegrp という名前のトンネル グループの PPP 接続に対して EAP を許可する例を示します。

```
hostname(config)# tunnel-group pppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group pppremotegrp ppp-attributes
hostname(config-ppp)# authentication eap
hostname(config-ppp)#
```

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。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**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。

authentication key eigrp

EIGRP パケットの認証をイネーブルにし、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **authentication key eigrp** コマンドを使用します。EIGRP 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。

authentication key eigrp *as-number key* **key-id** *key-id*

no authentication key eigrp *as-number*

構文の説明

as-number	認証する EIGRP プロセスの自律システム番号。これは、EIGRP ルーティング プロセスに設定されている値と同じにする必要があります。
key	EIGRP 更新を認証するキー。このキーには、最大 16 文字を含めることができます。
key-id *key-id*	キー ID 値。有効な値の範囲は 1 ～ 255 です。

デフォルト

EIGRP 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

EIGRP メッセージ認証をイネーブルにするには、**authentication mode eigrp** および **authentication key eigrp** コマンドの両方をインターフェイスに設定する必要があります。インターフェイスに設定された **authentication** コマンドを表示するには、**show running-config interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 に設定された EIGRP 認証の例を示します。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# authentication mode eigrp md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

関連コマンド

コマンド	説明
authentication mode eigrp	EIGRP 認証に使用する認証のタイプを指定します。

authentication mode eigrp

EIGRP 認証に使用する認証のタイプを指定するには、インターフェイス コンフィギュレーション モードで **authentication mode eigrp** コマンドを使用します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

authentication mode eigrp *as-num* **md5**

no authentication mode eigrp *as-num* **md5**

構文の説明

as-num	EIGRP ルーティング プロセスの自律システム番号です。
md5	EIGRP メッセージ認証に MD5 を使用します。

デフォルト

デフォルトでは、認証は提供されません。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

EIGRP メッセージ認証をイネーブルにするには、**authentication mode eigrp** および **authentication key eigrp** コマンドの両方をインターフェイスに設定する必要があります。インターフェイスに設定された **authentication** コマンドを表示するには、**show running-config interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 に設定された EIGRP 認証の例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# authentication mode eigrp 100 md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

関連コマンド

コマンド	説明
authentication key eigrp	EIGRP パケットの認証をイネーブルにし、認証キーを指定します。

authentication ms-chap-v1

L2TP over IPSec 接続で PPP の Microsoft CHAP Version 1 認証をイネーブルにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。このプロトコルは CHAP と類似していますが、CHAP のようなクリアテキスト パスワードではなく、暗号化されたパスワードのみをサーバが格納して比較するために、よりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

Microsoft CHAP Version 1 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。

authentication ms-chap-v2

no authentication ms-chap-v2

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	透過	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

この属性は、L2TP/IPSec トンネル グループ タイプのみに適用できます。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

authentication ms-chap-v2

L2TP over IPSec 接続に対して PPP の Microsoft CHAP Version 2 認証をイネーブルにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。このプロトコルは CHAP と類似していますが、CHAP のようなクリアテキスト パスワードではなく、暗号化されたパスワードのみをサーバが格納して比較するために、よりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

Microsoft CHAP バージョン 2 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。

authentication ms-chap-v1

no authentication ms-chap-v1

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	透過	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

この属性は、L2TP/IPSec トンネル グループ タイプのみに適用できます。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

authentication pap

L2TP over IPSec 接続に対して PPP の PAP 認証を許可するには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication pap** コマンドを使用します。このプロトコルは、認証時にクリアテキストのユーザ名とパスワードを渡すため、安全ではありません。

コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication pap

no authentication pap

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

デフォルトでは、PAP は認証プロトコルとして許可されていません。

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	透過	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

この属性は、L2TP/IPSec トンネル グループ タイプのみに適用できます。

例

次に、設定 ppp コンフィギュレーション モードで、ppremotegrp という名前のトンネル グループの PPP 接続に対して PAP を許可する例を示します。

```
hostname(config)# tunnel-group ppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group ppremotegrp ppp-attributes
hostname(config-ppp)# authentication pap
hostname(config-ppp)#
```

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。

コマンド	説明
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**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。

authentication-certificate

接続を確立している WebVPN クライアントから証明書を要求するには、webvpn コンフィギュレーション モードで **authentication-certificate** コマンドを使用します。クライアント証明書の要求をキャンセルするには、このコマンドの **no** 形式を使用します。

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

構文の説明

interface-name	接続を確立するために使用するインターフェイスの名前。使用可能なインターフェイス名は、次のとおりです。 • **inside**　GigabitEthernet0/1 インターフェイスの名前 • **outside**　GigabitEthernet0/0 インターフェイスの名前

デフォルト

- **authentication-certificate** コマンドを省略すると、クライアント証明書認証はディセーブルになります。
- interface-name を **authentication-certificate** コマンドで指定しない場合、デフォルトの interface-name は **inside** 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

このコマンドを有効にするには、WebVPN が対応するインターフェイスですでに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設定して名前を付けるには、**interface**、**IP address**、および **nameif** コマンドを使用します。

このコマンドは、WebVPN クライアント接続にのみ適用されます。ただし、**管理**接続のクライアント証明書認証を **http authentication-certificate** コマンドを使って指定することは、WebVPN をサポートしないプラットフォームも含めてすべてのプラットフォームで可能です。

セキュリティ アプライアンスは、PKI トラストポイントに対して証明書を検証します。証明書が検証に合格しない場合、次のいずれかのアクションが実行されます。

条件	実行されるアクション
セキュリティ アプライアンスに組み込まれているローカル CA がイネーブルでない場合。	セキュリティ アプライアンスは SSL 接続を閉じます。
ローカル CA はイネーブルであるが、AAA 認証がイネーブルでない場合。	セキュリティ アプライアンスは証明書を取得するために、クライアントをローカル CA の証明書登録ページにリダイレクトします。
ローカル CA と AAA 認証の両方がイネーブルの場合。	クライアントは AAA 認証ページにリダイレクトされます。設定されている場合、ローカル CA の登録ページのリンクもクライアントに表示します。

例

次に、外部インターフェイスの WebVPN ユーザ接続の証明書認証を設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
authentication（トンネル グループ webvpn コンフィギュレーション モード）	トンネル グループのメンバーは認証にデジタル証明書を使用する必要があることを指定します。
http authentication-certificate	認証にセキュリティ アプライアンスへの ASDM 管理接続用の証明書を使用することを指定します。
interface	接続の確立に使用するインターフェイスを設定します。
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 trust-point	SSL 証明書トラストポイントを設定します。

authentication-port

特定のホストの RADIUS 認証に使用するポート番号を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **authentication-port** コマンドを使用します。認証ポート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。このコマンドでは、認証機能を割り当てるリモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。

authentication-port *port*

no authentication-port

構文の説明

port	RADIUS 認証用のポート番号（1 ～ 65535）。

デフォルト

デフォルトでは、デバイスはポート 1645 で RADIUS をリッスンします（RFC 2058 に準拠）。ポートが指定されていない場合、RADIUS 認証のデフォルト ポート番号（1645）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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドのセマンティックが変更され、RADIUS サーバを含むサーバ グループでホストごとにサーバ ポートを指定できるようになりました。

使用上のガイドライン

RADIUS 認証サーバで 1645 以外のポートが使用されている場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、適切なポートをセキュリティ アプライアンスに設定する必要があります。

このコマンドは、RADIUS 用に設定されているサーバ グループに限り有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、認証ポートを 1650 に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドまたは ASDM ユーザ認証により指定されたサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
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。

authentication-server-group（imap4s、pop3s、smtps）

電子メール プロキシに使用する認証サーバのセットを指定するには、各モードで **authentication-server-group** コマンドを使用します。認証サーバ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。セキュリティ アプライアンスは、ユーザを認証してユーザ ID を確認します。

authentication-server-group *group_tag*

no authentication-server-group

構文の説明

group_tag	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。認証サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、認証サーバは設定されていません。

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	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—

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

AAA 認証を設定する場合は、この属性も設定する必要があります。設定しないと、認証は常に失敗します。

例

次に、「IMAP4SSVRS」という名前の認証サーバのセットを使用するように IMAP4S 電子メール プロキシを設定する例を示します。

```
hostname(config)# imap4s
hostname(config-imap4s)# authentication-server-group IMAP4SSVRS
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバを設定します。

authentication-server-group（トンネル グループ一般属性）

トンネル グループでユーザ認証に使用する AAA サーバ グループを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **authentication-server-group** コマンドを使用します。この属性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。

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]

no authentication-server-group [(*interface_name*)] *server_group*

構文の説明

interface_name	（任意）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。
server_group	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。

デフォルト

このコマンドのサーバ グループのデフォルト設定は **LOCAL** 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	透過	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	•	—	•	—	—

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。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
8.0(2)	このコマンドは、インターフェイス単位で IPSec 接続の認証を行えるように拡張されました。

使用上のガイドライン

この属性は、すべてのトンネル グループ タイプに適用できます。

認証サーバを設定するには **aaa-server** コマンドを使用し、設定済みの AAA サーバ グループにサーバを追加するには **aaa-server-host** コマンドを使用します。

例

次に、設定一般コンフィギュレーション モードで、remotegrp という名前の IPSec リモート アクセス トンネル グループに aaa-server456 という名前の認証サーバ グループを設定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成し、グループ固有の AAA サーバ パラメータとすべてのグループ ホストに共通の AAA サーバ パラメータを設定します。
aaa-server host	設定済みの AAA サーバ グループにサーバを追加し、ホスト固有の AAA サーバ パラメータを設定します。
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。
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。

authorization-dn-attributes

（注）　リリース 8.0(4) 以降このコマンドは廃止されました。このコマンドの代わりに **username-from-certificate** コマンドを使用します。

認可用のユーザ名として使用するプライマリ サブジェクト DN フィールドおよびセカンダリ サブジェクト DN フィールドを指定するには、各コンフィギュレーション モードで **authorization-dn-attributes** 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。

authorization-dn-attributes {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no authorization-dn-attributes

構文の説明

primary-attr	証明書から認可クエリー用の名前を生成するときに使用する属性を指定します。
secondary-attr	（任意）デジタル証明書から認可クエリー用の名前を生成するときにプライマリ属性と共に使用する追加の属性を指定します。
use-entire-name	セキュリティ アプライアンスでは、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。

デフォルト

プライマリ属性のデフォルト値は CN（一般名）です。

セカンダリ属性のデフォルト値は OU（組織の部門）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	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
7.2(1)	imap4s、pop3、および smtps コンフィギュレーション モードが追加されました。

使用上のガイドライン　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
CN	Common Name（一般名）：個人、システムなどの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
O	Organization（組織）：会社、団体、機関、連合などの名前。
L	Locality（地名）：組織が置かれている市または町。
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。
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。
EA	電子メール アドレス
T	肩書
N	名前
GN	名
SN	姓
I	イニシャル
GENQ	Generational Qualifier（世代修飾子）
DNQ	Domain Name Qualifier（ドメイン名修飾子）
UID	User Identifier（ユーザ識別子）
UPN	ユーザ プリンシパル名
SER	Serial Number（シリアル番号）
use-entire-name	DN 名全体を使用

例　次の例では、グローバル コンフィギュレーション モードで、remotegrp という IPSec リモート アクセス トンネル グループを作成し、デジタル証明書から認可クエリー用の名前を生成するために CN（Common Name; 一般名）をプライマリ属性として使用することを指定します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

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。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
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。

authorization-required

接続前にユーザが正常に認可されることを求めるには、各モードで **authorization-required** 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。

authorization-required

no authorization-required

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

authorization-required は、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	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

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。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
7.2(1)	webvpn コンフィギュレーション モードが imap4s、pop3s、および smtps コンフィギュレーション モードに置き換えられました。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループを介して接続するユーザに完全な DN に基づく認可を要求する例を示します。最初のコマンドでは、remotegrp という名前のリモート グループのトンネル グループ タイプを ipsec_ra（IPSec リモート アクセス）と設定しています。2 番めのコマンドで、指定したトンネル グループのトンネル グループ一般属性コンフィギュレーション モードを開始し、最後のコマンドで、指定したトンネル グループに認可が必要であることを指定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
authorization-dn-attributes	認可用のユーザ名として使用するプライマリおよびセカンダリ サブジェクト DN フィールドを指定します。
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。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
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。

authorization-server-group

WebVPN および電子メール プロキシに使用する認可サーバのセットを指定するには、各モードで **authorization-server-group** コマンドを使用します。認可サーバ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。セキュリティ アプライアンスでは、認可を使用して、ユーザに許可されているネットワーク リソースへのアクセス レベルを確認します。

authorization-server-group *group_tag*

no authorization-server-group

構文の説明

group_tag	設定済みの認可サーバまたはサーバ グループを指定します。認可サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、認可サーバは設定されていません。

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	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

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。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。

使用上のガイドライン

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

VPN 認可が LOCAL と定義されている場合、デフォルト グループ ポリシー DfltGrpPolicy に設定されている属性が適用されます。

例

次に、「POP3Spermit」という名前の許可サーバのセットを使用するように POP3S 電子メール プロキシを設定する例を示します。

```
hostname(config)# pop3s
```

```
hostname(config-pop3s)# authorization-server-group POP3Spermit
```

次に、設定一般コンフィギュレーション モードで、「remotegrp」という名前の IPSec リモート アクセス トンネル グループに「aaa-server78」という名前の許可サーバ グループを設定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバを設定します。
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。
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。

auth-prompt

セキュリティ アプライアンスを介したユーザ セッションの AAA チャレンジ テキストを指定または変更するには、グローバル コンフィギュレーション モードで **auth-prompt** コマンドを使用します。認証チャレンジ テキ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。

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

構文の説明

accept	Telnet 経由のユーザ認証を受け入れる場合、プロンプトとして *string* を表示します。
prompt	このキーワードの後に AAA チャレンジ プロンプトのストリングを入力します。
reject	Telnet 経由のユーザ認証を拒否する場合、プロンプトとして *string* を表示します。
string	235 文字または 30 単語（どちらか最初に達した方）までの英数字で構成されるストリング。特殊文字、スペース、および句読点を使用できます。疑問符を入力するか、または Enter キーを押すと、ストリングが終了します （疑問符はストリングに含まれます)。

デフォルト

認証プロンプトを指定しない場合は、次のようになります。

- FTP ユーザには `FTP authentication` が表示されます。
- HTTP ユーザには `HTTP Authentication` が表示されます。
- Telnet ユーザにはチャレンジ テキストが表示されません。

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	透過	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	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	セマンティックに小さな変更が加えられました。

使用上のガイドライン

auth-prompt コマンドを使用すると、TACACS+ サーバまたは RADIUS サーバからのユーザ認証が必要な場合に、セキュリティ アプライアンス経由の HTTP、FTP、および Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

Telnet からのユーザ認証が行われる場合、**accept** オプションと **reject** オプションを使用して、認証試行が AAA サーバによって受け入れられたか拒否されたかを示す各ステータス プロンプトを表示できます。

AAA サーバがユーザを認証すると、セキュリティ アプライアンスは **auth-prompt accept** テキスト（指定されている場合）をユーザに表示します。ユーザが認証されない場合は、**reject** テキスト（指定されている場合）を表示します。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。**accept** テキストと **reject** テキストは表示されません。

（注）　Microsoft Internet Explorer では、認証プロンプトに最大 37 文字表示されます。Telnet および FTP では、認証プロンプトに最大 235 文字表示されます。

例

次に、認証プロンプトを「Please enter your username and password」というストリングに設定する例を示します。

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

このストリングがコンフィギュレーションに追加されると、ユーザには次のように表示されます。

```
Please enter your username and password
User Name:
Password:
```

Telnet ユーザに対しては、セキュリティ アプライアンスが認証試行を受け入れたときに表示されるメッセージと拒否したときに表示されるメッセージを別々に指定できます。次に例を示します。

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

次に、認証に成功した場合の認証プロンプトを「You're OK.」というストリングに設定する例を示します。

```
hostname(config)# auth-prompt accept You're OK.
```

認証に成功すると、ユーザには次のメッセージが表示されます。

```
You're OK.
```

関連コマンド

コマンド	説明
clear configure auth-prompt	指定済みの認証プロンプト チャレンジ テキスト（ある場合）を削除し、デフォルト値に戻します。
show running-config auth-prompt	現在の認証プロンプト チャレンジ テキストを表示します。

auto-signon

クライアントレス SSL VPN 接続用のユーザ ログイン クレデンシャルを内部サーバに自動的に渡すようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション モード、webvpn グループ コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードのいずれかのモードで **auto-signon** コマンドを使用します。認証方式は、NTLM（NTLMv1 と NTLMv2 を含む）と HTTP 基本認証のいずれか一方、または両方にすることができます。特定のサーバへの自動サインオンをディセーブルにするには、元の **ip**、**uri**、および **auth-type** 引数を指定して、このコマンドの **no** 形式を使用します。すべてのサーバへの自動サインオンをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

auto-signon allow {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}

no auto-signon [**allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}]

構文の説明

all	NTLM と HTTP 基本認証の両方の方式を指定します。
allow	特定のサーバに対する認証をイネーブルにします。
auth-type	認証方式の選択をイネーブルにします。
basic	HTTP 基本認証方式を指定します。
ftp	FTP および CIFS 認証タイプを指定します。
ip	IP アドレスとマスクで認証先のサーバを特定することを指定します。
ip-address	*ip-mask* とともに使用して、認証先のサーバの IP アドレス範囲を特定します。
ip-mask	*ip-address* とともに使用して、認証先のサーバの IP アドレス範囲を特定します。
ntlm	NTLMv1 認証方式を指定します。
resource-mask	認証先のサーバの URI マスクを指定します。
uri	URI マスクで認証先のサーバを特定することを指定します。

デフォルト

デフォルトでは、この機能はすべてのサーバ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	透過	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（グローバル）	•	—	•	—	—
webvpn グループ ポリシー コンフィギュレーション	•	—	•	—	—
WebVPN ユーザ名コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(1)	NTLMv2 のサポートが追加されました。**ntlm** キーワードには、NTLMv1 と NTLMv2 の両方が含まれます。

使用上のガイドライン

auto-signon コマンドは、クライアントレス SSL VPN ユーザのためのシングル サインオン方式です。この方式では、ログイン クレデンシャル（ユーザ名とパスワード）を NTLM 認証と HTTP Basic 認証のいずれか一方または両方を使用する認証用の内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

auto-signon 機能は、webvpn コンフィギュレーション グループ ポリシー モード、webvpn コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。一般的な優先動作が適用されます。つまり、グループよりもユーザ名が優先され、グローバルよりもグループが優先されます。モードは、認証の目的範囲に基づいて選択します。

モード	スコープ
webvpn コンフィギュレーション	すべての WebVPN ユーザ（グローバル）
webvpn グループ コンフィギュレーション	グループ ポリシーで定義される WebVPN ユーザのサブセット
WebVPN ユーザ名コンフィギュレーション	個々の WebVPN ユーザ

例

次に、NTLM 認証を使用して、すべてのクライアントレス ユーザに自動サインオンを設定するコマンドの例を示します。認証先のサーバの IP アドレス範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

次に、HTTP 基本認証を使用して、すべてのクライアントレス ユーザに自動サインオンを設定するコマンドの例を示します。認証先のサーバは、URI マスク https://*.example.com/* で定義されています。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

次に、HTTP 基本認証または NTLM 認証を使用して、クライアントレス ユーザの ExamplePolicy グループに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定する例を示します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

次に、HTTP 基本認証を使用して、Anyuser という名前のユーザに自動サインオンを設定するコマンドの例を示します。認証先のサーバの IP アドレス範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
basic
```

関連コマンド

コマンド	説明
show running-config webvpn auto-signon	実行コンフィギュレーションの自動サインオンの割り当てを表示します。

auto-summary

ネットワークレベル ルートへのサブネット ルートの自動集約をイネーブルにするには、ルータ コンフィギュレーション モードで **auto-summary** コマンドを使用します。ルート集約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。

auto-summary

no auto-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

ルート集約は、RIP バージョン 1、RIP バージョン 2、および EIGRP 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	EIGRP のサポートが追加されました。

使用上のガイドライン

ルート集約により、ルーティング テーブルにおけるルーティング情報の量が少なくなります。

RIP バージョン 1 では、常に自動集約が使用されます。RIP バージョン 1 に対して自動集約をディセーブルにすることはできません。

RIP バージョン 2 を使用している場合は、**no auto-summary** コマンドを指定して、自動集約をオフにすることができます。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズをディセーブルにします。自動サマライズをディセーブルにすると、サブネットがアドバタイズされます。

EIGRP 集約ルートには、アドミニストレーティブ ディスタンス値 5 が割り当てられます。この値は設定できません。

実行コンフィギュレーションではこのコマンドの **no** 形式のみが表示されます。

例

次に、RIP ルート集約をディセーブルにする例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
hostname(config-router)# no auto-summary
```

次に、自動 EIGRP ルート集約をディセーブルにする例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# no auto-summary
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべての **router** コマンドとルータ コンフィギュレーション モード コマンドをクリアします。
router eigrp	EIGRP ルーティング プロセスをイネーブルにし、EIGRP ルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードを開始します。
show running-config router	実行コンフィギュレーション内の **router** コマンドとルータ コンフィギュレーション モード コマンドを表示します。

auto-update device-id

Auto Update Server で使用するセキュリティ アプライアンスのデバイス ID 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 **auto-update device-id** コマンドを使用します。デバイス ID を削除するには、このコマンドの **no** 形式を使用します。

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

構文の説明

hardware-serial	セキュリティ アプライアンスのハードウェア シリアル番号を使用して、デバイスを一意に識別します。
hostname	セキュリティ アプライアンスのホスト名を使用して、デバイスを一意に識別します。
ipaddress [*if_name*]	セキュリティ アプライアンスの IP アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは Auto Update Server との通信に使用するインターフェイスを使用します。別の IP アドレスを使用する場合は、*if_name* を指定します。
mac-address [*if_name*]	セキュリティ アプライアンスの MAC アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは Auto Update Server との通信に使用するインターフェイスの MAC アドレスを使用します。別の MAC アドレスを使用する場合は、*if_name* を指定します。
string *text*	テキスト ストリングを指定して、デバイスを Auto Update Server に対して一意に識別します。

デフォルト

デフォルト ID はホスト名です。

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	透過	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	•	•	•	—	—

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。

例

次に、デバイス ID をシリアル番号に設定する例を示します。

```
hostname(config)# auto-update device-id hardware-serial
```

関連コマンド

auto-update poll-period	Auto Update Server からのアップデートをセキュリティ アプライアンス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、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server の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。

auto-update poll-at

セキュリティ アプライアンスが Auto Update Server をポーリングする特定の日時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 **auto-update poll-at** コマンドを使用します。セキュリティ アプライアンスが Auto Update Server をポーリングするようにスケジューリングした日時のうち、指定した日時をすべて削除するには、このコマンドの **no** 形式を使用します。

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

no auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

構文の説明

days-of-the-week	任意の 1 つの曜日（Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday）または曜日の組み合わせ。その他の指定可能な値は、daily（月曜日から日曜日まで）、weekdays（月曜日から金曜日まで）、および weekend（土曜日と日曜日）です。
randomize *minutes*	指定した開始日時の後、不定期にポーリングする期間を指定します。1 ～ 1439 分です。
retry_count	Auto Update Server への接続の初回試行が失敗した場合に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続試行の間隔を指定します。デフォルトは 5 分です。指定できる範囲は 1 ～ 35791 分です。
time	ポーリングを開始する時刻を HH:MM 形式で指定します。たとえば、8:00 は 8:00 AM で、20:00 は 8:00 PM 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	透過	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	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(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

auto-update poll-at コマンドでは、更新をポーリングする時刻を指定します。**randomize** オプションをイネーブルにすると、最初の *time* の時刻から指定した期間（分単位）内に、ポーリングが不定期に実行されます。**auto-update poll-at** および **auto-update poll-period** コマンドは、同時に使用できません。いずれか 1 つのみを設定できます。

例

次の例で、セキュリティ アプライアンスは、毎週金曜日と土曜日の午後 10 時から午後 11 時までの間、不定期に Auto Update Server を ポーリングします。セキュリティ アプライアンスは、サーバに接続できない場合、10 分間隔で 2 回接続を試行します。

```
hostname(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
hostname(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

関連コマンド

auto-update device-id	Auto Update Server で使用するためのセキュリティ アプライアンス 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セキュリティ アプライアンスが確認する頻度を設定します。
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、セキュリティ アプライアンス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。
management-access	セキュリティ アプライアンスの内部管理インターフェイスへのアクセスをイネーブルにします。
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。

auto-update poll-period

セキュリティ アプライアンスが Auto Update Server からの更新を確認する頻度を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-period** コマンドを使用します。パラメータ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。

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

構文の説明

poll_period	Auto Update Server をポーリングする頻度を分単位（1 ～ 35791）で指定します。デフォルトは 720 分（12 時間）です。
retry_count	Auto Update Server への接続の初回試行が失敗した場合に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続試行の間隔を分単位（1 ～ 35791）で指定します。デフォルトは 5 分です。

デフォルト

デフォルトのポーリング期間は、720 分（12 時間）です。

Auto Update Server への最初の接続試行に失敗した場合に再接続を試行するデフォルトの回数は 0 です。

接続試行のデフォルト間隔は 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	透過	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	•	•	•	—	—

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

auto-update poll-at および **auto-update poll-period** コマンドは、同時に使用できません。いずれか 1 つのみを設定できます。

例

次に、ポーリング期間を 360 分に、再試行回数を 1 回に、再試行間隔を 3 分に設定する例を示します。

```
hostname(config)# auto-update poll-period 360 1 3
```

関連コマンド

auto-update device-id	Auto Update Server で使用するためのセキュリティ アプライアンス デバイス ID 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、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server の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。

auto-update server

Auto Update Server 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 **auto-update 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。セキュリティ アプライアンスは、定期的に Auto Update Server にアクセスして、コンフィギュレーション、オペレーティング システム、および ASDM の更新がないか調べます。

auto-update server *url* [**source** *interface*] [*verify-certificate*]

no auto-update server *url* [**source** *interface*] [*verify-certificate*]

構文の説明

interface	要求を Auto Update Server に送信するときに使用するインターフェイスを指定します。
url	次の構文を使用して、Auto Update Server の場所を指定します。 **http**[**s**]**:**[[*user:password@*]*location* [*:port*]] / *pathname*
verify_certificate	Auto Update Server から返された証明書を検証します。

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	透過	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	•	•	•	—	—

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。
7.2(1)	複数のサーバをサポートできるようにコマンドが変更されました。

使用上のガイドライン

自動更新用に複数のサーバを設定できます。更新を確認するときに、最初のサーバに接続しますが、接続に失敗した場合は、次のサーバに接続します。これは、すべてのサーバを試行するまで続行されます。どのサーバにも接続できなかった場合は、auto-update poll-period が接続を再試行するように設定されていれば、最初のサーバから順に接続が再試行されます。

自動更新機能を正しく動作させるには、**boot system configuration** コマンドを使用して、有効なブート イメージを指定する必要があります。同様に、**asdm image** コマンドを使用して、自動更新で ASDM ソフトウェア イメージを更新する必要があります。

source *interface* 引数で指定されたインターフェイスが **management-access** コマンドで指定されたインターフェイスと同じである場合、Auto Update Server への要求は VPN トンネルを介して送信されます。

例

次に、Auto Update Server の URL を設定し、インターフェイス outside を指定する例を示します。

```
hostname(config)# auto-update server http://10.1.1.1:1741/ source outside
```

関連コマンド

auto-update device-id	Auto Update Server で使用するためのセキュリティ アプライアンス 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セキュリティ アプライアンスが確認する頻度を設定します。
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、セキュリティ アプライアンス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。
management-access	セキュリティ アプライアンスの内部管理インターフェイスへのアクセスをイネーブルにします。
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。

auto-update timeout

Auto Update Server へのアクセスのタイムアウト期間を設定するには、グローバル コンフィギュレーション モードで **auto-update timeout** コマンドを使用します。タイムアウト期間内に Auto Update Server へのアクセスが行われなかった場合、セキュリティ アプライアンスはセキュリティ アプライアンスを通過するすべてのトラフィックを停止します。タイムアウトを設定すると、セキュリティ アプライアンスに最新のイメージとコンフィギュレーションが保持されます。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。

auto-update timeout *period*

no auto-update timeout [*period*]

構文の説明

period	タイムアウト期間を分単位（1 ～ 35791）で指定します。デフォルトは 0 で、タイムアウトがないことを意味します。タイムアウトを 0 に設定することはできません。タイムアウトを 0 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。

デフォルト

デフォルトのタイムアウトは 0 で、セキュリティ アプライアンスはタイムアウトしないよう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	透過	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	•	•	•	—	—

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

タイムアウト状態は、システム ログ メッセージ 201008 でレポートされます。

例

次に、タイムアウトを 24 時間に設定する例を示します。

```
hostname(config)# auto-update timeout 1440
```

関連コマンド

auto-update device-id	Auto Update Server で使用するためのセキュリティ アプライアンス 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セキュリティ アプライアンス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。
clear configure auto-update	Auto Update Server の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。