pr - pz

- pre-fill-username （3 ページ）
- preempt （5 ページ）
- prefix-list （7 ページ）
- prefix-list description （11 ページ）
- prefix-list sequence-number （13 ページ）
- prf （15 ページ）
- primary （17 ページ）
- priority（クラス） （19 ページ）
- priority（クラスタ グループ） （22 ページ）
- priority（vpn ロード バランシング） （25 ページ）
- priority-queue （27 ページ）
- privilege （30 ページ）
- profile （34 ページ）
- prompt （38 ページ）
- propagate sgt （41 ページ）
- protocol （43 ページ）
- protocol-enforcement （46 ページ）
- protocol http （48 ページ）
- protocol ldap （50 ページ）
- protocol-object （52 ページ）
- protocol scep （54 ページ）
- protocol shutdown （56 ページ）
- protocol-violation （57 ページ）
- proxy-auth （59 ページ）
- proxy-auth_map sdi （60 ページ）
- proxy-bypass （62 ページ）
- proxy-ldc-issuer （65 ページ）
- proxy paired （67 ページ）
- proxy-server（廃止予定） （69 ページ）
- proxy single-arm （71 ページ）

- ptp domain （73 ページ）
- ptp enable （75 ページ）
- ptp mode （77 ページ）
- public-key （79 ページ）
- publish-crl （81 ページ）
- pwd （83 ページ）

pre-fill-username

認証と認可で使用するクライアント証明書からユーザー名を抽出できるようにするには、トンネルグループ webvpn 属性モードで **pre-fill-username** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

pre-fill-username { **client** | **clientless** }
no pre-fill-username

構文の説明

client **ssl-client**	この機能を AnyConnect VPN クライアント接続でイネーブルにします。9.8(1) 以降では **client** キーワードを使用してください。
clientless	この機能をクライアントレス接続でイネーブルにします。

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。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
9.8(1)	**ssl-client** キーワードが **client** に変更されました。

使用上のガイドライン

pre-fill-username コマンドは、**username-from-certificate** コマンドで指定された証明書フィールドから抽出されたユーザー名を、ユーザー名またはパスワード認証のユーザー名として使用できるようにします。証明書機能からこの事前充填ユーザー名を使用するには、両方のコマンドを設定する必要があります。

この機能を有効にするには、トンネルグループ一般属性モードで **username-from-certificate** コマンドを入力する必要もあります。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成し、SSL VPN クライアントの認証または認可クエリーの名前をデジタル証明書から取得する必要があることを指定する例を示します。

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

関連コマンド

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

preempt

フェールオーバーグループが優先ユニットでアクティブになるようにするには、フェールオーバー グループ コンフィギュレーション モードで **preempt** コマンドを使用します。プリエンプションを削除するには、このコマンドの **no** 形式を使用します。

preempt [*delay*]
no preempt [*delay*]

構文の説明

seconds ピアがプリエンプション処理されるまでの待機時間（秒数）。有効な値は、1 ～ 1200 秒です。

コマンド デフォルト

デフォルトでは遅延はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバー グループを優先ユニットでアクティブにする **preempt** コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバー グループが最初に起動するユニットでアクティブになるように変更されました。

使用上のガイドライン

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

トに強制されない限り、2 番めのユニットではアクティブになりません。フェールオーバーグループが **preempt** コマンドで設定される場合、指定されたユニットでフェールオーバーグループが自動的にアクティブになります。

（注） ステートフル フェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバーグループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どちらのフェールオーバーグループも **preempt** コマンドで待機時間が 100 秒に設定されているため、グループは、ユニットが使用可能になってから 100 秒後に自動的にその優先ユニットでアクティブになります。

```
ciscoasa(config)# failover group 1

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

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
primary	設定対象のフェールオーバー グループに対するフェールオーバー ペア プライオリティにおける、プライマリ ユニットを指定します。
secondary	設定対象のフェールオーバー グループに対するフェールオーバー ペア プライオリティにおける、セカンダリ ユニットを指定します。

prefix-list

OSPFv2、EIGRP、およびBGPプロトコルでは、グローバルコンフィギュレーションモードで **prefix-list** コマンドを使用します。プレフィックスリストの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。

prefix-list*prefix-list-name*[**seq***seq_num*]{ **permit** | **deny** } *network*/*len*[**ge***min_value*][**le***max_value*]
no prefix-list *prefix-list-name* [**seq** *seq_num*] { **permit** | **deny** } *network* / *len* [**ge** *min_value*] [**le** *max_value*]

構文の説明

/	*network* 値と *len* 値との間に必要な区切り文字。
deny	一致した条件へのアクセスを拒否します。
ge *min_value*	（任意）照会されるプレフィックスの最小の長さを指定します。*min_value* 引数の値は、*len* 引数の値よりも大きく、*max_value* 引数が存在する場合はそれ以下である必要があります。
le *max_value*	（任意）照会されるプレフィックスの最大の長さを指定します。*max_value* 引数の値は、*min_value* 引数が存在する場合はその値以上、*min_value* 引数が存在しない場合は *len* 引数よりも大きい値にする必要があります。
len	ネットワーク マスクの長さ。有効な値は、0 ～ 32 です。
network	ネットワーク アドレス。
permit	一致した条件へのアクセスを許可します。
prefix-list-name	プレフィックス リストの名前。プレフィックス リスト名にスペースを含めることはできません。
seq *seq_num*	（任意）作成するプレフィックスリストに指定されたシーケンス番号を適用します。

コマンド デフォルト

シーケンス番号を指定しない場合、プレフィックスリストの先頭エントリにはシーケンス番号 5 が割り当てられ、その後のエントリのシーケンス番号は 5 ずつ増えていきます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチコンテキストモードのサポートが追加されました。
9.2(1)	BGP のサポートが追加されました。

使用上のガイドライン

prefix-list コマンドは、ABR のタイプ 3 LSA フィルタリングコマンドです。ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されると、指定したプレフィックスのみがエリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックスリストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。ASA では、プレフィックスリストの先頭、つまりシーケンス番号が最も小さいエントリから検索が開始されます。一致が見つかると、ASA はリストの残りを検索しません。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

デフォルトでは、シーケンス番号は自動的に生成されます。自動生成されるシーケンス番号は、**no prefix-list sequence-number** コマンドで抑制できます。シーケンス番号は、5 ずつ増分されます。プレフィックスリストで生成される最初のシーケンス番号は5です。そのリストの次のエントリにはシーケンス番号 10 が設定され、以降も同様に設定されます。あるエントリに値を指定し、その後のエントリに値を指定しない場合、生成されるシーケンス番号は指定された値から5ずつ増分されます。たとえば、プレフィックスリストの最初のエントリのシーケンス番号を 3 と指定し、その後シーケンス番号を指定しないで 2 つのエントリを追加した場合、これら2つエントリに対して自動的に生成されるシーケンス番号は、8および13となります。

ge キーワードおよび **le** キーワードを使用して、*network*/*len* 引数よりも具体的なプレフィックスに対して一致するプレフィックス長の範囲を指定できます。**ge** または **le** キーワードが指定されていない場合、完全一致であると見なされます。**ge** キーワードのみが指定されている場合の範囲は、*min_value* ～ 32 です。**le** キーワードのみが指定されている場合の範囲は、*len* ～ *max_value* です。

min_value 引数および *max_value* 引数の値は、次の条件を満たす必要があります。

len < *min_value* <= *max_value* <= 32

プレフィックスリストから特定の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。プレフィックスリストを削除するには、**clear configure prefix-list** コマンドを使用します。clear **configure prefix-list** コマンドを使用すると、関連する **prefix-list description** コマンド（ある場合）も構成から削除されます。

例

次に、デフォルト ルート 0.0.0.0/0 を拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0
```

次に、プレフィックス 10.0.0.0/8 を許可する例を示します。

```
ciscoasa(config)# prefix-list abc permit 10.0.0.0/8
```

次に、プレフィックス 192/8 のルートで最大 24 ビットのマスク長を許可する例を示します。

```
ciscoasa(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

次に、プレフィックス 192/8 のルートで 25 ビットよりも大きいマスク長を拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

次に、すべてのアドレス空間で 8 ～ 24 ビットのマスク長を許可する例を示します。

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

次に、すべてのアドレス空間で25ビットよりも大きいマスク長を拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

次に、プレフィックス 10/8 のすべてのルートを拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

次に、プレフィックス 192.168.1/24 のルートで 25 ビットよりも大きいすべてのマスクを拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

次に、プレフィックス 0/0 のすべてのルートを許可する例を示します。

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

関連コマンド

コマンド	説明
clear configure prefix-list	実行コンフィギュレーションから **prefix-list** コマンドを削除します。
prefix-list description	プレフィックス リストの説明を入力できます。
prefix-list sequence-number	プレフィックス リストのシーケンス番号付けをイネーブルにします。

コマンド	説明
show running-config prefix-list	実行コンフィギュレーションの **prefix-list** コマンドを表示します。

prefix-list description

プレフィックスリストに説明を追加するには、グローバル コンフィギュレーション モードで **prefix-list description** コマンドを使用します。プレフィックスリストの説明を削除するには、このコマンドの **no** 形式を使用します。

prefix-list*prefix-list-name***description***text*
no prefix-list *prefix-list-name* **description** [*text*]

構文の説明

prefix-list-name	プレフィックス リストの名前。
text	プレフィックスリストの説明テキスト。最大80文字を入力できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

prefix-list および **prefix-list description** コマンドは、特定のプレフィックスリスト名に対して、任意の順序で入力できます。プレフィックスリストの説明を入力する前に、プレフィックスリストを作成する必要はありません。**prefix-list description** コマンドは、コマンドの入力順に関係なく、構成内の関連するプレフィックスリストの前の行に必ず記述されます。

すでに説明が入力されているプレフィックス リスト エントリに対して **prefix-list description** コマンドを入力した場合、新しい説明によって元の説明が置き換えられます。

このコマンドの **no** 形式を使用する場合、テキストの説明を入力する必要はありません。

例

次に、MyPrefixList という名前のプレフィックス リストの説明を追加する例を示します。**show running-config prefix-list** コマンドを実行すると、プレフィックスリストの説明が実行コンフィギュレーションに追加されていても、プレフィックスリスト自体は設定されていないことが示されます。

```
ciscoasa(config)# prefix-list MyPrefixList description A sample prefix list description
ciscoasa(config)# show running-config prefix-list
!
prefix-list MyPrefixList description A sample prefix list description
!
```

関連コマンド

コマンド	説明
clear configure prefix-list	実行コンフィギュレーションから **prefix-list** コマンドを削除します。
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーションの **prefix-list** コマンドを表示します。

prefix-list sequence-number

プレフィックスリストのシーケンス番号付けを有効にするには、グローバル コンフィギュレーション モードで **prefix-list sequence-number** コマンドを使用します。プレフィックスリストのシーケンス番号付けを無効にするには、このコマンドの **no** 形式を使用します。

prefix-list sequence-number

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

プレフィックス リストのシーケンス番号付けは、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。このコマンドの **no** 形式が構成内にある場合、シーケンス番号（手動設定した番号を含む）は構成内の **prefix-list** コマンドから削除され、プレフィックスリストの新しいエントリにシーケンス番号は割り当てられません。

プレフィックスリストのシーケンス番号付けがイネーブルの場合、デフォルトの番号付け方式（5 で始まり、番号が 5 ずつ増分される）を使用して、プレフィックス リストのすべてのエントリにシーケンス番号が割り当てられます。番号付けがディセーブルになる前に、シーケンス番号がプレフィックスリストのエントリに手動で割り当てられた場合、手動で割り当てられた番号が復元されます。自動番号付けがディセーブルのときに手動で割り当てたシーケンス番号も復元されます。ただし、番号付けがディセーブルの間、これらのシーケンス番号は表示されません。

例

次に、プレフィックス リストのシーケンス番号付けをディセーブルにする例を示します。

```
ciscoasa(config)# no prefix-list sequence-number
```

関連コマンド

コマンド	説明
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーションの **prefix-list** コマンドを表示します。

prf

AnyConnect IPsec 接続に使用する IKEv2 セキュリティ アソシエーション（SA）の疑似乱数関数（PRF）を指定するには、IKEv2 ポリシー コンフィギュレーション モードで prf コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの no 形式を使用します。

prf { **md5** | **sha** | **sha256** | **sha384** | **sha512** }
no prf { **md5** | **sha** | **sha256** | **sha384** | **sha512** }

構文の説明

md5	MD5 アルゴリズムを指定します。
sha	（デフォルト）セキュア ハッシュ アルゴリズム SHA 1 を指定します。
sha256	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha384	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha512	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。

コマンド デフォルト

デフォルトは **sha**（SHA 1）です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。crypto ikev2 policy コマンドを入力後、**prf** コマンドを使用して、SA で使用されるすべての暗号化アルゴリズムのキー関連情報の構築に使用する疑似乱数関数を選択します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
8.4(2)	SHA 2 をサポートするために、sha256、sha384、および sha512 の各キーワードが追加されました。

例

次に、IKEv2 ポリシー コンフィギュレーション モードを開始し、PRF を MD5 に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# prf md5
```

関連コマンド

コマンド	説明
encryption	AnyConnect IPsec 接続に対して IKEv2 SA の暗号化アルゴリズムを指定します。
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
integrity	AnyConnect IPsec 接続に対して IKEv2 SA の ESP 整合性アルゴリズムを指定します。
ライフタイム	AnyConnect IPsec 接続に対して IKEv2 SA の SA ライフタイムを指定します。

primary

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

primary
no primary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバー グループを優先ユニットでアクティブにする **preempt** コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバー グループが最初に起動するユニットでアクティブになるように変更されました。

使用上のガイドライン

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

ループが **preempt** コマンドで設定される場合、指定されたユニットでフェールオーバーグループが自動的にアクティブになります。

例

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

```
ciscoasa(config)# failover group 1

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

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

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

priority（クラス）

QoS プライオリティキューイングを有効にするには、クラス コンフィギュレーション モードで **priority** コマンドを使用します。Voice over IP（VoIP）のように遅延を許容できない重要なトラフィックでは、常に最低レートで送信されるように低遅延キューイング（LLQ）のトラフィックを特定できます。プライオリティの要件を削除するには、このコマンドの **no** 形式を使用します。

（注） このコマンドは、ASA サービス モジュールではサポートされていません。

priority
no priority

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や変数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

ASA は、次の 2 つのタイプのプライオリティキューイングをサポートしています。

- 標準プライオリティキューイング：標準プライオリティキューイングではインターフェイスでLLQプライオリティキューを使用しますが（**priority-queue** コマンドを参照）、他のすべてのトラフィックは「ベストエフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになる

と、以降のパケットはキューに入ることができず、すべてドロップされます。これはテールドロップと呼ばれます。キューがいっぱいになるのを避けるには、キューのバッファサイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。

- 階層型プライオリティキューイング：階層型プライオリティキューイングは、トラフィック シェーピング キュー（**shape** コマンド）を有効にしているインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。階層型プライオリティ キューイングについては、次のガイドラインを参照してください。
- プライオリティ パケットは常にシェープ キューの先頭に格納されるので、常に他の非プライオリティ キュー パケットよりも前に送信されます。
- プライオリティ トラフィックの平均レートがシェープ レートを超えない限り、プライオリティ パケットがシェープ キューからドロップされることはありません。
- IPsec-encrypted パケットの場合、DSCP または先行する設定に基づいてのみトラフィックを照合することができます。
- プライオリティ トラフィック分類では、IPsec-over-TCP はサポートされません。

モジュラ ポリシー フレームワークを使用した QoS の設定

プライオリティ キューイングをイネーブルにするには、モジュラー ポリシー フレームワークを使用します。標準プライオリティ キューイングまたは階層型プライオリティ キューイングを使用できます。

標準プライオリティ キューイングの場合は、次の作業を実行します。

1.class-map：プライオリティキューイングを実行するトラフィックを指定します。

2.policy-map：各クラスマップに関連付けるアクションを指定します。

- **a.class**：アクションを実行するクラスマップを指定します。
- **b.priority**：クラスマップのプライオリティキューイングを有効にします。

3.service-policy：ポリシーマップをインターフェイスごとに、またはグローバルに割り当てます。

階層型プライオリティ キューイングの場合は、次の作業を実行します。

1.class-map：プライオリティキューイングを実行するトラフィックを指定します。

2.policy-map（プライオリティキューイングの場合）：各クラスマップに関連付けるアクションを指定します。

- **a.class**：アクションを実行するクラスマップを指定します。

- **b.priority**：クラスマップのプライオリティキューイングを有効にします。ポリシー マップを階層的に使用する場合は、このポリシー マップに priority コマンドだけを含めることができます。

3.policy-map（トラフィックシェーピングの場合）：**class-default** クラスマップに関連付けるアクションを指定します。

- **a.class class-default**：アクションを実行する **class-default** クラスマップを指定します。
- **b.shape**：トラフィックシェーピングをクラスマップに適用します。
- **c.service-policy**：プライオリティキューイングをシェーピングされたトラフィックのサブセットに適用できるように、**priority** コマンドを設定したプライオリティ キューイング ポリシー マップを呼び出します。

4.service-policy：ポリシーマップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、ポリシー マップ コンフィギュレーション モードでの **priority** コマンドの例を示します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class firstclass
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

関連コマンド

class	トラフィック分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシーマップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のポリシーマップ コンフィギュレーションをすべて表示します。

priority（クラスタ グループ）

ASA クラスタにおけるこのユニットのマスターユニット選定に関するプライオリティを設定するには、クラスタ コンフィギュレーション モードで **priority** コマンドを使用します。プライオリティを削除するには、このコマンドの **no** 形式を使用します。

priority *priority_number*
no priority [*priority_number*]

構文の説明

priority_number	マスター ユニット選定用に、このユニットのプライオリティを 1 ～ 100 の範囲内で設定します。1 が最高のプライオリティです。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. ユニットに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのユニットは選定要求を 3 秒間隔でブロードキャストします。

2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。

3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。

（注） 最高のプライオリティを持つユニットが複数ある場合は、クラスタユニット名、次にシリアル番号を使用してマスターが決定されます。

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスターユニットになることはありません。既存のマスターユニットは常にマスターのままです。ただし、マスター ユニットが応答を停止すると、その時点で新しいマスター ユニットが選定されます。

（注） **cluster master unit** コマンドを使用して、手動で強制的に特定のユニットをマスターにできます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。中央集中型機能のリストについては、設定ガイドを参照してください。

例

次に、プライオリティ を 1（最高）に設定する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# priority 1
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。
enable (cluster group)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルスチェック機能（ユニットのヘルスモニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。

コマンド	説明
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンクインターフェイスの最大伝送ユニットを指定します。
priority (cluster group)	マスター ユニット選定のこのユニットのプライオリティを設定します。

priority（vpn ロード バランシング）

仮想ロードバランシングクラスタに参加するローカルデバイスのプライオリティを設定するには、VPN ロードバランシングモードで **priority** コマンドを使用します。デフォルトのプライオリティ指定に戻すには、このコマンドの **no** 形式を使用します。

priority *priority*
no priority

構文の説明

priority このデバイスに割り当てるプライオリティ（1～10の範囲）。

コマンド デフォルト

デフォルトのプライオリティは、デバイスのモデル番号によって異なります。

モデル番号	デフォルトのプライオリティ
5520	5
5540	7

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシングモードを開始する必要があります。

このコマンドは、仮想ロード バランシング クラスタに参加するローカル デバイスのプライオリティを設定します。

プライオリティは、1（最低）～ 10（最高）の範囲の整数である必要があります。

プライオリティは、VPN ロード バランシング クラスタ内でクラスタのマスターまたはプライマリ デバイスになるデバイスを決定する方法の1つとして、マスター選出プロセスで使用されます。マスター選出プロセスの詳細については、CLI 設定ガイドを参照してください。

プライオリティ指定を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。

例

次に、現在のデバイスのプライオリティを9に設定する **priority** コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードを開始します。

priority-queue

priority コマンドで使用するインターフェイスで標準プライオリティキューを作成するには、グローバル コンフィギュレーション モードで **priority-queue** コマンドを使用します。キューを削除するには、このコマンドの **no** 形式を使用します。

（注） このコマンドは、ASA 5580 の 10 ギガビット イーサネットインターフェイスではサポートされていません（10 ギガビット イーサネットインターフェイスは、ASA 5585-X でプライオリティキュー用にサポートされています）。また、このコマンドは、ASA 5512-X ～ ASA 5555-X の管理インターフェイスではサポートされていません。このコマンドは、ASA サービスモジュールではサポートされていません。

priority-queue *interface-name*
no priority-queue *interface-name*

構文の説明

interface-name	プライオリティキューを有効にする物理インターフェイスの名前を指定します。ASA 5505 や ASASM の場合は、VLAN インターフェイスの名前を指定します。

コマンド デフォルト

デフォルトでは、プライオリティ キューイング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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(3)/8.4(1)	ASA 5585-X 用に 10 ギガビット イーサネット インターフェイスのサポートが追加されました。

使用上のガイドライン

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

ASA は、次の 2 つのタイプのプライオリティキューイングをサポートしています。

- 標準プライオリティキューイング：標準プライオリティキューイングでは、インターフェイスで **priority-queue** コマンドを使用して作成する LLQ プライオリティキューを使用しますが、他のすべてのトラフィックは「ベストエフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これはテールドロップと呼ばれます。キューがいっぱいになるのを防ぐために、キューのバッファサイズを増やせます（**queue-limit** コマンド）。送信キューに入れることができるパケットの最大数も微調整できます（**tx-ring-limit** コマンド）。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。
- 階層型プライオリティキューイング：階層型プライオリティ キューイングは、トラフィック シェーピング キューがイネーブルなインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。

（注） ASA 5505 に限り、1 つのインターフェイスでプライオリティ キューを設定すると、他のすべてのインターフェイスの同じコンフィギュレーションが上書きされます。つまり、最後に適用されたコンフィギュレーションだけがすべてのインターフェイスに存在することになります。また、プライオリティ キュー コンフィギュレーションは、1 つのインターフェイスから削除すると、すべてのインターフェイスから削除されます。この問題を回避するには、priority-queue コマンドを 1 つのインターフェイスにのみ設定します。queue-limit コマンドと tx-ring-limit コマンドの両方またはそのいずれかの設定を、さまざまなインターフェイスで異なる設定にする必要がある場合、任意の 1 つのインターフェイスで、すべての queue-limit のうちで最大の値と、すべての tx-ring-limit のうちで最小の値を使用します（CSCsi13132）。

例

次に、test という名前のインターフェイスに対してプライオリティ キューを設定し、キュー制限に 30,000 パケット、送信キュー制限に 256 パケットを指定する例を示します。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 30000
ciscoasa(priority-queue)# tx-ring-limit 256
ciscoasa(priority-queue)#
```

関連コマンド

コマンド	説明
queue-limit	プライオリティ キューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。

コマンド	説明
tx-ring-limit	イーサネット送信ドライバのキューに任意のタイミングで入れることができるパケットの最大数を設定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
clear configure priority-queue	現在のプライオリティ キュー コンフィギュレーションを削除します。
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、このコマンドは現在のすべてのプライオリティキュー、queue-limit、および tx-ring-limit コンフィギュレーションの値を表示します。

privilege

コマンド認可（ローカル、RADIUS、および LDAP（マッピング）のみ）で使用するコマンド特権レベルを設定するには、グローバル コンフィギュレーション モードで **privilege** コマンドを使用します。構成を拒否するには、このコマンドの **no** 形式を使用します。

privilege ［ **show** ｜ **clear** ｜ **configure** ］ **level** *level* ［ **mode** *cli_mode* ］ **command** *command*
no privilege ［ **show** ｜ **clear** ｜ **configure** ］ **level** *level* ［ **mode** *cli_mode* ］ **command** *command*

構文の説明

clear	（任意）コマンドの clear 形式に対してのみ特権を設定します。**clear**、**show**、または **configure** キーワードを使用しない場合は、コマンドのすべての形式が影響を受けます。
command *command*	設定するコマンドを指定します。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルは個別に設定できません。
configure	（任意）コマンドの configure 形式に対してのみ特権を設定します。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。**clear**、**show**、または **configure** キーワードを使用しない場合は、コマンドのすべての形式が影響を受けます。
level *level*	特権レベルを指定します。有効な値は、0 ～ 15 です。特権レベルの番号が小さいと、特権レベルが低くなります。

mode *cli_mode*	（オプション）ユーザー EXEC/特権 EXEC モード、グローバル コンフィギュレーション モード、特定のコマンドのコンフィギュレーション モードなど、複数の CLI モードでコマンドを入力できる場合、それらのモードの特権レベルを個別に設定することができます。モードを指定しない場合は、コマンドのすべてのバージョンで同じレベルが使用されます。次のモードを参照してください。 • **exec**：ユーザー EXEC モードと特権 EXEC モードの両方を指定します。 • **configure**：**configure terminal** コマンドを使用してアクセスされるグローバル コンフィギュレーション モードを指定します。 • *command_config_mode*：コマンドのコンフィギュレーション モードを指定します。グローバル コンフィギュレーション モードまたは別のコマンドのコンフィギュレーション モードでコマンド名を指定してアクセスできます。 たとえば、**mac-address** コマンドは、グローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードの両方で入力できます。mode キーワードを使用して、各モードのレベルを個別に設定できます。 このコマンドを使用してコマンドのレベルを設定することはできません。
show	（任意）コマンドの show 形式に対してのみ特権を設定します。**clear**、**show**、または **configure** キーワードを使用しない場合は、コマンドのすべての形式が影響を受けます。

コマンド デフォルト

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のコマンドはすべて、レベル 15 です。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。そうしないと、ユーザーはコンフィギュレーション モードを開始できません。

すべての特権レベルを表示する方法については、**show running-config all privilege all** コマンドを参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	Cisco VSA CVPN3000-Privilege-Level を使用する RADIUS ユーザーのサポートが追加されました。 **ldap map-attributes** コマンドを使用して LDAP 属性を CVPN3000-Privilege-Level にマッピングすると、LDAP ユーザーがサポートされます。

使用上のガイドライン

privilege コマンドを使用すると、**aaa authorization command LOCAL** コマンドを設定するときに、ASA コマンドの特権レベルを設定できます。このコマンドで **LOCAL** キーワードを使用する場合でも、このキーワードによってローカル、RADIUS、および LDAP（マッピング）認可が有効になります。

例

たとえば、**filter** コマンドの形式は次のとおりです。

- **filter**（**configure** オプションで表現）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。たとえば、それぞれの形式を別々に設定するには、次のように指定します。

```
ciscoasa(config)# privilege
 show
 level
 5
 command
 filter
ciscoasa(config)# privilege
```

```
 clear
 level
 10
 command
 filter
ciscoasa(config)# privilege
 cmd
 level
 10
 command
 filter
```

また、すべてのフィルタ コマンドを同じレベルに設定できます。

```
ciscoasa(config)# privilege
 level
 5
 command
 filter
```

show privilege コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザー EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
ciscoasa(config)# privilege cmd level 0 mode exec command enable
ciscoasa(config)# privilege cmd level 15 mode configure command enable
ciscoasa(config)# privilege show level 15 mode configure command enable
```

次に、2 つのモードの **mac-address** コマンドの例を示します。show、clear、および cmd のレベルを個別に設定しています。

```
ciscoasa(config)# privilege cmd level 10 mode configure command mac-address
ciscoasa(config)# privilege cmd level 15 mode interface command mac-address
ciscoasa(config)# privilege clear level 10 mode configure command mac-address
ciscoasa(config)# privilege clear level 15 mode interface command mac-address
ciscoasa(config)# privilege show level 2 mode configure command mac-address
ciscoasa(config)# privilege show level 2 mode interface command mac-address
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

profile

Call Home プロファイルを作成または編集するには、Call Home コンフィギュレーション モードで **profile** コマンドを使用します。設定済みの 1 つまたはすべての Call Home プロファイルを削除するには、このコマンドの **no** 形式を使用して、1 つまたはすべてのプロファイルを指定します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力します。

profile *profile-name*
no profile { *profile-name* | **all** }

構文の説明

profile-name	プール名（最大 20 文字）。
all	すべての設定済みプロファイルが含まれます。

コマンド デフォルト

デフォルトプロファイル **Cisco TAC** が提供されました。デフォルト プロファイルには、事前定義されたモニター対象グループ（診断、環境、インベントリ、コンフィギュレーション、テレメトリ）のセットと、事前定義された宛先電子メールおよび HTTPS URL があります。デフォルト プロファイルは、Smart Call Home を初めて設定するときに自動的に作成されます。宛先電子メールは callhome@cisco.com で、宛先 URL は https://tools.cisco.com/its/service/oddce/services/DDCEService です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.2(2)	キーワード all が追加されました。
9.3(2)	スマート ソフトウェア ライセンシング用に **License** プロファイルが追加されました。
9.6(2)	**destination address http** の reference-identity オプションが導入されました。

使用上のガイドライン

次のコマンドは、イン プロファイル コンフィギュレーション モードで使用されます。

プロファイルの有効化または無効化

Call Home プロファイルを有効にするには、Call Home プロファイル コンフィギュレーション モードで **active** コマンドを使用します。Call Home プロファイルを無効にするには、Call Home プロファイル コンフィギュレーション モードで **no active** コマンドを使用します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力して、**profile** コマンドを入力します。デフォルトではイネーブルになっています。

active

no active

Profile コマンドのデフォルトへの設定

Call Home プロファイル設定をデフォルト値に設定するには、Call Home プロファイル コンフィギュレーション モードで default コマンドを使用します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力して、**profile** コマンドを入力します。このモードから Call Home コンフィギュレーション モード設定をリセットすることもできます。すべての Call Home プロファイルおよび全般設定を確認およびリセットする方法については、コマンドヘルプ（**default ?**）を参照してください。

default {**activedestinationemail-subjectsubscribe-to-alert-group**}

宛先タイプ、アドレス、および設定

Smart Call Home メッセージ受信者の宛先アドレス、参照アイデンティティ、メッセージ形式、およびトランスポート方式を設定するには、Call Home プロファイル コンフィギュレーション モードで **destination** コマンドを使用します。宛先パラメータを削除、またはパラメータをデフォルトにリセットするには、**no destination** コマンドまたは **default** コマンドを使用します。

デフォルト メッセージ形式は XM、デフォルト メッセージ サイズは 5 MB（0 にすると無制限）、デフォルトのトランスポート方式は電子メールです。事前に設定された参照アイデンティティを指定する必要があります。これは、接続時に Call Home サーバーの証明書を検証するために使用されます。これは、HTTP 宛先にのみ適用されます。

destination address {**e-mail** *e-mail-address***http** *http-url*}
no destination address {**e-mailhttp** [**all**]}
destination address http *http-url* **reference-identity** *ref-id-name*
no destination address http *http-url* **reference-identity** *ref-id-name*
destination address {**e-mail** *e-mail-address***http** *http-url*} **msg-format** {**short-textlong-textxml**}
no destination address {**e-mail** *e-mail-address***http** *http-url*} **msg-format** {**short-textlong-textxml**}
destination message-size-limit *max-size*
no destination message-size-limit *max-size*
destination preferred-msg-format {**short-textlong-textxml**}
no destination preferred-msg-format {**short-textlong-textxml**}
destination transport-method {**e-mailhttp**}
no destination transport-method {**e-mailhttp**}

電子メールの件名の設定

Call Home 電子メールの件名のプレフィックスまたはサフィックスを設定するには、Call Home プロファイル コンフィギュレーション モードで **email-subject** コマンドを使用します。これらのフィールドをクリアするには、**no email-subject** コマンドを使用します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力して、**profile** コマンドを入力します。

email-subject {**appendprepend**} *chars*
no email-subject {**appendprepend**} *chars*

アラートグループへの登録

アラートグループに登録するには、Call Homeプロファイル コンフィギュレーション モードで **ubscribe-to-alert-group** コマンドを使用します。これらのサブスクリプションをクリアするには、no s**ubscribe-to-alert-group** コマンドを使用します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力して、**profile** コマンドを入力します。

- [no] subscribe-to-alert-group alert-group-name [severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging}]：指定した重大度レベルのグループのイベントにサブスクライブします。alert-group-name：有効な値は、syslog、diagnostic、environment、または threat です。
- [no] subscribe-to-alert-group syslog [{severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging} | message start [-end]}]：重大度レベルまたはメッセージ ID のある syslog にサブスクライブします。start-[end]：1 つの syslog メッセージ ID またはある範囲の syslog メッセージ ID。

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

- [no] subscribe-to-alert-group inventory [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]：インベントリイベントにサブスクライブします。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。
- [no] subscribe-to-alert-group configuration [export full | minimum] [periodic {daily | month day_of_month | weekly day_of_week [hh：mm]]：設定イベントにサブスクライブします。full：実行コンフィギュレーション、スタートアップ コンフィギュレーション、機能リスト、アクセスリストの要素数、およびマルチモードのコンテキスト名をエクスポートするコンフィギュレーション。minimum：機能リスト、アクセスリスト内の要素数、およびマ

ルチモードのコンテキスト名だけをエクスポートするコンフィギュレーション。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。

- [no] subscribe-to-alert-group telemetry periodic {hourly | daily | monthly day_of_month | weekly day_of_week [hh:mm]：テレメトリ定期イベントをサブスクライブします。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。
- [no] subscribe-to-alert-group snapshot periodic {interval minutes | hourly [mm] | daily | monthly day_of_month |weekly day_of_week [hh:mm]}：スナップショット定期イベントにサブスクライブします。minutes：分単位の間隔。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。

関連コマンド

コマンド	説明
call-home	ユーザーを Call Home コンフィギュレーション モードにします。
show call-home	Call Home コンフィギュレーション情報を表示します。
reference-identity	参照アイデンティティ オブジェクトを設定します。

prompt

CLIプロンプトをカスタマイズするには、グローバル コンフィギュレーション モードでprompt コマンドを使用します。デフォルトのプロンプトに戻すには、このコマンドの no 形式を使用します。

prompt { [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]
no prompt [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]

構文の説明

cluster-unit	クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
context	（マルチ モードのみ）現在のコンテキストを表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。プライオリティは **failover lan unit** コマンドを使用して設定します。
state	ユニットのトラフィック通過状態またはロールを表示します。 フェールオーバーの場合、**state** キーワードに対して次の値が表示されます。 • [act]：フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。 • stby：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailove]：フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。これは、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 クラスタリングの場合、**state** キーワードに対して次の値が表示されます。 • control node • data node たとえば、**prompt hostname cluster-unit state** と設定して「ciscoasa/cl2/data node>」と表示された場合、ホスト名は ciscoasa、ユニット名は cl2、状態名は data node です。

コマンド デフォルト

デフォルトのプロンプトはホスト名です。マルチコンテキストモードでは、ホスト名の後に現在のコンテキスト名（*hostname* /*context*）が続きます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.0(1)	**cluster-unit** オプションが追加されました。クラスタリング用に **state** キーワードが更新されました。
9.19(1)	クラスタリングの場合、**state** 表示が **master** と **slave** から **control node** と **data node** に変更されました。

使用上のガイドライン

キーワードを入力する順序によって、プロンプト内の要素の順序が決まります。要素はスラッシュ（/）で区切ります。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

プロンプトに情報を追加する機能により、複数のモジュールが存在する場合にログインしている ASA を一目で確認することができます。この機能は、フェールオーバー時に、両方の ASA に同じホスト名が設定されている場合に便利です。

例

次に、フェールオーバー用のプロンプトで使用可能なすべての要素を表示する例を示します。

```
ciscoasa(config)# prompt hostname context slot state priority
```

プロンプトが次のストリングに変化します。

```
ciscoasa/admin/pri/act(config)#
```

関連コマンド

コマンド	説明
clear configure prompt	設定したプロンプトをクリアします。

コマンド	説明
show running-config prompt	設定したプロンプトを表示します。

propagate sgt

インターフェイスでのセキュリティグループタグ（**sgt**）の伝達を有効にするには、CTS 手動インターフェイス コンフィギュレーション モードで **propagate sgt** コマンドを使用します。インターフェイスでのセキュリティグループタグ（**sgt**）の伝達を無効にするには、このコマンドの **no** 形式を使用します。

propagate sgt
no propagate sgt

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

伝搬はデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、CTS レイヤ 2 SGT インポジションのセキュリティ グループ タグの伝播をイネーブルまたはディセーブルにできます。

制約事項

- 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイスおよび冗長インターフェイスでのみサポートされます。
- BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。

例

次に、レイヤ 2 SGT インポジションのインターフェイスをイネーブルにし、SGT の伝播は行わないように設定する例を示します。

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# no propagate sgt
```

関連コマンド

コマンド	説明
cts manual	レイヤ 2 SGT インポジションをイネーブルにし、CTS 手動インターフェイス コンフィギュレーション モードを開始します。
policy static sgt	手動で設定された CTS リンクにポリシーを適用します。

protocol

IKEv2接続のIPsecプロポーザルに使用するプロトコルタイプと暗号化タイプを指定するには、IPsecプロポーザル コンフィギュレーション モードで **protocol** コマンドを使用します。プロトコルおよび暗号化タイプを削除するには、このコマンドの no 形式を使用します。

protocol esp { **encryption** { **des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **aes-gmac** | **aes-gmac-192** | **aes-gmac-256** | **null** } | **integrity** { **md5** | **sha-1** | **sha-256** | **sha-384** | **sha-512** | **null** }
no protocol esp { **encryption** { **des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **aes-gmac** | **aes-gmac-192** | **aes-gmac-256** | **null** } | **integrity** { **md5** | **sha-1** | **sha-256** | **sha-384** | **sha-512** | **null** }

構文の説明

esp	カプセル化セキュリティ ペイロード（ESP）IPsec プロトコルを指定します（現在、唯一サポートされている IPsec のプロトコルです）。
des	56 ビット DES-CBC 暗号化を ESP に対して指定します。
3des	（デフォルト）トリプル DES 暗号化アルゴリズムを ESP に対して指定します。
aes	AES と 128 ビット キー暗号化を ESP に対して指定します。
aes-192	AES と 192 ビット キー暗号化を ESP に対して指定します。
aes-256	AES と 256 ビット キー暗号化を ESP に対して指定します。
aes-gcm	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gcm-192	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gcm-256	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gmac	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gmac-192	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gmac-256	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
null	ESP に暗号化を使用しません。
integrity	IPsec プロトコルの整合性アルゴリズムを指定します。
md5	ESP の整合性保護のために MD5 アルゴリズムを指定します。
sha-1	（デフォルト）は、ESP の整合性保護のために米国連邦情報処理標準（FIPS）で定義されたセキュア ハッシュ アルゴリズム（SHA）SHA-1 を指定します。
sha-256	IPsec 整合性アルゴリズムとして使用するアルゴリズムを指定します。
sha-384	IPsec 整合性アルゴリズムとして使用するアルゴリズムを指定します。

sha-512	IPsec 整合性アルゴリズムとして使用するアルゴリズムを指定します。
null	AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合に選択します。

コマンド デフォルト

IPsec プロポーザルのデフォルトの設定は、暗号化タイプが 3DES で、整合性タイプが SHA-1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	AES-GCM または AES-GMAC アルゴリズムのサポートが追加されました。IPsec 整合性アルゴリズムとして使用するアルゴリズムを選択できるようになりました。

使用上のガイドライン

IKEv2 IPsec プロポーザルには、暗号化タイプと整合性タイプを複数設定できます。このコマンドで指定したタイプの中から、必要なタイプをピアで選択することができます。

AES-GMC/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

例

次に、proposal_1 という IPsec プロポーザルを作成する例を示します。ESP 暗号化タイプとして DES と 3DES を設定し、整合性保護のために暗号化アルゴリズム MD5 と SHA-1 を指定しています。

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal proposal_1
ciscoasa(config-ipsec-proposal)# protocol ESP encryption des 3des
ciscoasa(config-ipsec-proposal)# protocol ESP integrity md5 sha-1
```

関連コマンド

コマンド	説明
crypto ikev2 enable	IPsec ピアの通信に使用するインターフェイスで ISAKMP IKEv2 ネゴシエーションをイネーブルにします。

コマンド	説明
crypto ipsec ikev2 ipsec-proposal	IPsec プロポーザルを作成し、IPsec プロポーザル コンフィギュレーションモードを開始します。このコンフィギュレーション モードで、プロポーザルに対して暗号化タイプと整合性タイプを複数指定できます。
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。
crypto map set transform-set	クリプトマップエントリで使用するトランスフォームセットを指定します。
crypto dynamic-map set transform-set	ダイナミック クリプトマップエントリで使用するトランスフォーム セットを指定します。
show running-config crypto map	クリプト マップの設定内容を表示します。
show running-config crypto dynamic-map	ダイナミック クリプトマップのコンフィギュレーションを表示します。

protocol-enforcement

ドメイン名、ラベル長、形式チェック（圧縮およびループポインタのチェックを含む）を有効にするには、パラメータ コンフィギュレーション モードで **protocol-enforcement** コマンドを使用します。プロトコルの強制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。

protocol-enforcement
no protocol-enforcement

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

プロトコルの強制は、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** コマンドを定義していない場合でも、**inspect dns** コマンドを設定していれば有効にできます。無効にするには、ポリシーマップ コンフィギュレーションで **no protocol-enforcement** コマンドを明示的に指定する必要があります。**inspect dns** が設定されていない場合、NAT リライトは実行されません。

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

状況によっては、コマンドがディセーブルであっても、プロトコルの強制が実行されます。これは、DNS リソース レコードの分類、NAT、TSIG チェックなど、他の目的で DNS リソース レコードの解析が必要なときに発生します。

例

次に、DNS インスペクション ポリシー マップ内でプロトコルの強制をイネーブルにする方法を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-enforcement
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

protocol http

CRL を取得するための許可された配布ポイントプロトコルとして HTTP を指定するには、ca-crl コンフィギュレーション モードで **protocol http** コマンドを使用します。CRL 取得方法として許可した HTTP を削除するには、このコマンドの **no** 形式を使用します。

protocol http
no protocol http

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの設定は、HTTP 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する場合は、HTTP ルールをパブリック インターフェイス フィルタに適用してください。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして HTTP を許可する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol http
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。

コマンド	説明
crypto ca trustpoint	トラストポイントコンフィギュレーションモードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。
protocol scep	CRL の取得方法として SCEP を指定します。

protocol ldap

CRL を取得するための配布ポイントプロトコルとして LDAP を指定するには、ca-crl コンフィギュレーション モードで **protocol ldap** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した LDAP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol ldap
no protocol ldap

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの設定は、LDAP 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして LDAP を許可する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol ldap
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。

コマンド	説明
crypto ca trustpoint	トラストポイントコンフィギュレーションモードを開始します。
protocol http	CRL の取得方法として HTTP を指定します。
protocol scep	CRL の取得方法として SCEP を指定します。

protocol-object

プロトコル オブジェクト グループにプロトコル オブジェクトを追加するには、プロトコル コンフィギュレーション モードで protocol-object コマンドを使用します。ポートオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

protocol-object *protocol*
no protocol-object *protocol*

構文の説明

protocol	プロトコルの名前または番号。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

protocol-object コマンドは、**object-group** コマンドとともに使用して、プロトコル コンフィギュレーション モードでプロトコルオブジェクトを定義します。

IP プロトコルの名前や番号は、*protocol* 引数を使用して指定できます。udp プロトコル番号は 17、tcp プロトコル番号は 6、egp プロトコル番号は 47 です。

例

次に、プロトコル オブジェクトを定義する例を示します。

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol)# protocol-object udp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# exit
ciscoasa(config)# object-group protocol proto_grp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# group-object proto_grp_1
ciscoasa(config-protocol)# exit
ciscoasa(config)#
```

関連コマンド

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

protocol scep

CRL を取得するための配布ポイントプロトコルとして SCEP を指定するには、crl コンフィギュレーション モードで **protocol scep** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した SCEP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol scep
no protocol scep

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの設定は、SCEP 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして SCEP を許可する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol scep
ciscoasa(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。

コマンド	説明
crypto ca trustpoint	トラストポイントコンフィギュレーションモードを開始します。
protocol http	CRL の取得方式として HTTP を指定します。
protocol ldap	CRL の取得方法として LDAP を指定します。

protocol shutdown

いずれのインターフェイスとの隣接関係も形成できず IS-IS LSP データベースをクリアさせるために IS-IS プロトコルを無効にするには、ルータ ISIS コンフィギュレーション モードで **protocol shutdown** コマンドを使用します。IS-IS プロトコルを再び有効にするには、このコマンドの **no** 形式を使用します。

protocol shutdown
no protocol shutdown

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、既存の IS-IS コンフィギュレーション パラメータを削除することなく特定のルーティング インスタンスの IS-IS プロトコルをディセーブルにすることができます。**protocol shutdown** コマンドを入力した場合、IS-IS プロトコルは引き続き ASA 上で動作し、ユーザーは現在の IS-IS 設定を使用できますが、IS-IS はいずれのインターフェイスでも隣接関係を確立せず、IS-IS LSP データベースもクリアします。

特定のインターフェイスで IS-IS プロトコルを無効にするには、**isis protocol shutdown** コマンドを使用します。

例

次に、特定のルーティング インスタンスの IS-IS プロトコルをディセーブルにする例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# protocol shutdown
```

関連コマンド

protocol-violation

HTTP および NetBIOS インスペクションでプロトコル違反が発生したときのアクションを定義するには、パラメータ コンフィギュレーション モードで **protocol-violation** 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。

protocol-violation action [**drop** [**log**] | **log**]
no protocol-violation action [**drop** [**log**] | **log**]

構文の説明

drop	プロトコルに準拠しないパケットをドロップすることを指定します。
ログ	プロトコル違反をログに記録することを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、HTTP または NetBIOS ポリシーマップで設定できます。HTTP または NetBIOS パーサーが HTTP または NetBIOS メッセージの最初の数バイトで有効なメッセージを検出できない場合、syslog が発行されます。たとえば、チャンク エンコーディングの形式が不正であるためにメッセージを解析できない場合に、このような状況が発生します。

例

次に、ポリシーマップにおけるプロトコル違反に対するアクションを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation action drop
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシーマップ コンフィギュレーションをすべて表示します。

proxy-auth

トンネルグループにフラグを付けて特定のプロキシ認証のトンネルグループとして設定するには、webvpn コンフィギュレーション モードで **proxy-auth** コマンドを使用します。

proxy-auth [**sdi**]

構文の説明

sdi	RADIUS/TACACS SDI プロキシ メッセージをネイティブ SDI ディレクティブに解析します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

proxy-auth コマンドは、AAA サーバープロキシ認証のテキストメッセージのネイティブ プロトコル ディレクティブへの解析を有効にする場合に使用します。

proxy-auth_map sdi

RADIUS プロキシサーバーから返された RADIUS チャレンジメッセージをネイティブ SDI メッセージにマッピングするには、AAA サーバー コンフィギュレーション モードで **proxy-auth_map sdi** コマンドを使用します。

proxy-auth_map sdi [**sdi_message**] [**radius_challenge_message**]

構文の説明

radius_challenge_message	特定の SDI メッセージのマッピングに使用する RADIUS チャレンジ メッセージを指定します。次のいずれかを指定できます。 • new-pin-meth：新しい PIN 方式。デフォルトは「Do you want to enter your own pin」 • new-pin-reenter：新しい PIN の再入力。デフォルトは「Reenter PIN:」 • new-pin-req：新しい PIN の要求。デフォルトは「Enter your new Alpha-Numerical PIN」 • new-pin-sup：新しい PIN の提供。デフォルトは「Please remember your new PIN」 • new-pin-sys-ok：新しい PIN の受理。デフォルトは「New PIN Accepted」 • next-ccode-and-reauth：トークン変更時の再認証。デフォルトは「new PIN with the next card code」 • next-code：PIN なしのトークンコードの指定。デフォルトは「Enter Next PASSCODE」 • ready-for-sys-pin：システムで生成された PIN の受け入れ。デフォルトは「ACCEPT A SYSTEM GENERATED PIN」
sdi_message	ネイティブ SDI メッセージを指定します。

コマンド デフォルト

ASA のデフォルトのマッピングは、Cisco ACS のデフォルト設定（システム管理、構成、RSA SecureID のプロンプトなど）と対応しており、RSA 認証マネージャのデフォルト設定とも同期されています。

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。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

RADIUS プロキシからの RADIUS チャレンジメッセージの解析とマッピングを有効にするには、トンネル グループ コンフィギュレーション モードで **proxy-auth** コマンドを有効にする必要があります。これにより、デフォルトのマッピングの値が使用されます。デフォルトのマッピングの値は、**proxy-auth_map** コマンドを使用して変更できます。

リモートユーザーは、セキュアクライアント で ASA に接続し、RSA SecurID トークンを使用して認証を試みます。RADIUS プロキシサーバーを使用して、認証に関する SDI サーバーと通信するように ASA を設定できます。

認証の間に、RADIUS サーバは ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。このメッセージテキストは、ASA が SDI サーバーと直接通信している場合と RADIUS プロキシを経由して通信している場合では異なります。

そのため、セキュアクライアント にネイティブ SDI サーバーとして認識させるために、ASA は RADIUS サーバーからのメッセージを解釈する必要があります。また、SDI メッセージは SDI サーバで設定可能であるため、ASA のメッセージテキストの全体または一部が、SDI サーバのメッセージ テキストと一致する必要があります。一致しない場合、リモート クライアント ユーザに表示されるプロンプトが、認証中に必要とされるアクションに対して適切でない場合があります。この場合、セキュアクライアント が応答できずに認証が失敗する場合があります。

関連コマンド

コマンド	説明
proxy-auth	RADIUS プロキシからの RADIUS チャレンジ メッセージの解析とマッピングをイネーブルにします。

proxy-bypass

コンテンツの最低限の書き換えを実行し、書き換えるコンテンツのタイプ（外部リンクや XML）を指定するように ASA を設定するには、webvpn コンフィギュレーション モードで **proxy-bypass** コマンドを使用します。プロキシのバイパスを無効にするには、このコマンドの **no** 形式を使用します。

proxy-bypass interface *interface name* { **port** *port number* | **path-mask** *path mask* } **target** *url* [**rewrite** { **link** | **xml** | **none**] }
no proxy-bypass interface *interface name* { **port** *port number* | **path-mask** *path mask* } **target** *url* [**rewrite** { **link** | **xml** | **none**] }

構文の説明

ホスト	トラフィックの転送先ホストを示します。ホストの IP アドレスまたはホスト名を使用します。
interface	プロキシ バイパス用の ASA インターフェイスを示します。
interface name	ASA インターフェイスを名前で指定します。
link	絶対外部リンクの書き換えを指定します。
none	書き換えを指定しません。
path-mask	一致パターンを指定します。
path-mask	照合対象として正規表現を含むことができるパターンを指定します。次のワイルドカードを使用できます。 *****：完全一致。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 ? ：少なくとも 1 文字を一致させます。 [!seq]：順序に関係なく、任意の文字を含みます。 [seq]：順序も含め、任意の文字を含みます。 最大 128 バイトです。
port	プロキシ バイパス用に予約されているポートを示します。
port number	プロキシ バイパス用に予約されているポート（大きい番号）を指定します。ポートの範囲は 20000 ～ 21000 です。1 つのプロキシ バイパス ルールのみにポートを使用できます。
rewrite	（任意）書き換え用の追加ルール（なし、または XML やリンクの組み合わせ）を指定します。
target	トラフィックの転送先リモート サーバーを示します。

url	URL を **http(s)://***fully_qualified_domain_name*[:*port*] という形式で入力します。最大 128 バイトです。別のポートを指定しない限り、HTTP のポートは 80、HTTPS のポートは 443 です。
xml	書き換える XML コンテンツを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

プロキシ バイパスは、コンテンツの書き換えを最小限に実行して、アプリケーションおよび Web リソースの動作を向上させるために使用します。proxy-bypass コマンドは、ASA を通過する特定の Web アプリケーションの処理方法を決定します。

このコマンドは複数回使用できます。エントリを設定する順序は重要ではありません。インターフェイスとパスマスク、またはインターフェイスとポートにより、プロキシバイパスルールが一意に指定されます。

パスマスクではなくポートを使用してプロキシバイパスを設定する場合、ネットワーク構成によっては、それらのポートが ASA にアクセスできるようにするために、ファイアウォール構成を変更する必要があります。この制限を回避するには、パスマスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスは、URL で .com や .org、またはその他のタイプのドメイン名の後に続く全体です。たとえば、www.example.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.example.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、*（ワイルドカード）を /hr* のように使用して、コマンドを複数回使用しないようにできます。

例

次に、WebVPN インターフェイス上のプロキシバイパス用にポート 20001 を使用するように ASA を設定する例を示します。HTTP とそのデフォルトポート 80 を使用してトラフィックを example.com に転送し、XML コンテンツを書き換えます。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface webvpn port 20001 target http://example.com rewrite xml
```

次に、外部インターフェイスでのプロキシバイパス用にパスマスク mypath/* を使用するように ASA を設定する例を示します。HTTP とそのデフォルトポート 443 を使用してトラフィックを example.com に転送し、XML およびリンクコンテンツを書き換えます。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface outside path-mask /mypath/* target https://example.com rewrite
xml,link
```

関連コマンド

コマンド	説明
apcf	特定のアプリケーションに使用する非標準のルールを指定します。
rewrite	トラフィックが ASA を通過するかどうかを決定します。

proxy-ldc-issuer

TLS プロキシ ローカル ダイナミック証明書を発行するには、クリプト CA トラストポイント コンフィギュレーション モードで proxy-ldc-issuer コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

proxy-ldc-issuer
no proxy-ldc-issuer

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

TLS プロキシ ローカル ダイナミック証明書を発行するには、proxy-ldc-issuer コマンドを使用します。proxy-ldc-issuer コマンドは、クリプト トラストポイントにローカル CA としてのロールを付与して LDC を発行します。クリプト ca トラストポイント コンフィギュレーション モードからアクセスできます。

proxy-ldc-issuer コマンドは、TLS プロキシのダイナミック証明書を発行するトラストポイントに、ローカル CA の役割を定義します。このコマンドは、「自己登録」を使用するトラストポイントでのみ設定できます。

例

次に、内部ローカル CA を作成し、電話用の LDC を署名する例を示します。このローカル CA は、proxy-ldc-issuer がイネーブルな標準の自己署名トラストポイントとして作成されます。

```
ciscoasa(config)# crypto ca trustpoint ldc_server
```

```
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# proxy-ldc-issuer
ciscoasa(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
ciscoasa(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
ciscoasa(config-ca-trustpoint)# keypair ldc_signer_key
ciscoasa(config)# crypto ca enroll ldc_server
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

proxy paired

Azure Gateway Load Balancer（GWLB）の Azure 上の ASA Virtual のペアプロキシモードに VNI インターフェイスを指定するには、インターフェイス コンフィギュレーション モードで **proxy paired** コマンドを使用します。プロキシを削除するには、このコマンドの **no** 形式を使用します。

proxy paired
no proxy paired

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.19(1)	このコマンドが追加されました。

使用上のガイドライン

Azure サービスチェーンでは、ASA Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

例

次の例では、Azure GWLB の VNI 1 インターフェイスを設定します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
external-port	外部 VXLAN ポートを設定します。
external-segment-id	VNI インターフェイスの VXLAN 外部セグメント ID を指定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
internal-port	内部 VXLAN ポートを設定します。
internal-segment-id	VNI インターフェイスの VXLAN 内部セグメント ID を指定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

proxy-server（廃止予定）

IP 電話の構成ファイルの <proxyServerURL> タグの下に書き込まれる、電話プロキシ機能に対して HTTP プロキシを設定するには、電話プロキシ コンフィギュレーション モードで **proxy-server** コマンドを使用します。電話プロキシから HTTP プロキシ構成を削除するには、このコマンドの **no** 形式を使用します。

proxy-server address *ip_address* [*listen_port*] **interface** *ifc*
no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

構文の説明

interface *ifc*	ASA で HTTP プロキシが常駐するインターフェイスを指定します。
ip_address	HTTP プロキシの IP アドレスを指定します。
listen_port	HTTP プロキシのリスニング ポートを指定します。指定しない場合、デフォルトは 8080 になります。

コマンド デフォルト

リッスン ポートを指定しない場合、ポートはデフォルトで 8080 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。

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

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モードコマンドとともに廃止されました。

使用上のガイドライン

電話プロキシのプロキシサーバー コンフィギュレーション オプションを設定すると、DMZ または外部ネットワークで HTTP プロキシを使用できます。これらのネットワークでは、電話機上のサービスについてすべての IP フォンの URL がこのプロキシ サーバーに誘導されます。この設定では、非セキュアな HTTP トラフィックに対応します。このようなトラフィックは社内ネットワークに入ることはできません。

入力する *ip_address* は、IP フォンおよび HTTP プロキシ サーバーの配置場所に基づくグローバル IP アドレスにする必要があります。

プロキシサーバーが DMZ 内にあり、IP 電話がネットワークの外部にある場合、ASA は NAT ルールの存在を確認するためにルックアップを実行し、グローバル IP アドレスを使用して構成ファイルに書き込みます。

ASA はホスト名を IP アドレスに解決できる場合（DNS ルックアップが設定されている場合など）、そのホスト名を IP アドレスに解決するため、*ip_address* 引数にホスト名を入力できます。

デフォルトでは、エンタープライズ パラメータの下に設定された電話の URL パラメータは、URL 内で FQDN を使用しています。HTTP プロキシ用の DNS lookup で FQDN が解決されない場合は、IP アドレスを使用するようにこれらのパラメータを変更する必要があります。

プロキシ サーバー URL が IP フォンのコンフィギュレーション ファイルに正しく書き込まれたかどうかを確認するには、[Settings] > [Device Configuration] > [HTTP configuration] > [Proxy Server URL] で IP フォンの URL をチェックします。

電話プロキシでは、プロキシ サーバーに対するこの HTTP トラフィックを検査しません。

ASA が IP 電話と HTTP プロキシサーバーのパス内にある場合は、既存のデバッグ手法（syslog やキャプチャなど）を使用して、プロキシサーバーをトラブルシューティングします。

電話プロキシが使用中の場合は、プロキシサーバーを 1 つだけ設定できます。ただし、プロキシ サーバーを設定した後に IP 電話にコンフィギュレーション ファイルをダウンロードした場合は、IP 電話を再起動して、プロキシサーバーのアドレスが記載されたコンフィギュレーション ファイルが取り込まれるようにする必要があります。

例

次に、**proxy-server** コマンドを使用して電話プロキシ用に HTTP プロキシサーバーを設定する例を示します。

```
ciscoasa(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

proxy single-arm

VXLAN VNI インターフェイスの single-arm プロキシを指定するには、インターフェイス コンフィギュレーション モードで **proxy single-arm** コマンドを使用します。プロキシを無効にするには、このコマンドの **no** 形式を使用します。

proxy single-arm
no proxy single-arm

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドが追加されました。

使用上のガイドライン

AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。ASA 仮想 は、分散データプレーン（ゲートウェイ ロードバランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。このユースケースでは、VNI インターフェイスを single-arm プロキシとして設定する必要があります。**same-security-traffic permit intra-interface** も有効にして、トラフィックが VTEP 送信元インターフェイスを U ターンできるようにしてください。

例

次に、VNI インターフェイスを single-arm プロキシとして設定する例を示します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif geneve1000
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

```
ciscoasa(config-if)# proxy single-arm
ciscoasa(config)# same-security-traffic permit intra-interface
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
encapsulation geneve	NVE インスタンスを Geneve カプセル化に設定します。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。

ptp domain

ISA 3000 上のすべての PTP ポートのドメイン番号を指定するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **ptp domain** コマンドを使用します。ドメイン番号は 0 ～ 255 で、デフォルト値は 0 です。設定したドメインとは異なるドメイン上で受け取ったパケットは、通常のマルチキャストパケットのように処理され、PTP 処理は行われません。ドメイン番号をデフォルト値の 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。

ptp domain *domain_num*
no ptp domain

（注） このコマンドは、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

domain *domain_num*	ISA 3000 上の PTP 対応のすべてのポートにドメイン番号を指定します。

コマンド デフォルト

デフォルトの **ptp domain** 番号は、0 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

ptp domain コマンドは、グローバル コンフィギュレーション モードでも使用できます。

例

次に、**ptp domain** コマンドを使用して、PTP ドメイン番号を 127 に設定する例を示します。

```
ciscoasa# ptp domain 127
```

関連コマンド

コマンド	説明
show ptp port	PTPインターフェイス/ポート情報を表示します。

ptp enable

ISA 3000 上のインターフェイスで PTP を有効にするには、インターフェイス コンフィギュレーション モードで **ptp enable** コマンドを使用します。PTP が有効になるモードは、**ptp mode** コマンドで指定します。インターフェイスで PTP を無効にするには、このコマンドの **no** 形式を使用します。インターフェイスとの間で着信および発信する PTP パケットは、通常のマルチキャスト パケットと同様に扱われます。

ptp enable
no ptp enable

（注） このコマンドは、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、トランスペアレント モードのすべての ISA 3000 インターフェイスで PTP がイネーブルになっています。ルーテッドモードでは、PTP パケットがデバイスを通過できるようにするために必要な設定を追加する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを入力できるのは、インターフェイス コンフィギュレーション モードのみです。

このコマンドは物理インターフェイスのみで使用できます。サブインターフェイス、その他の仮想インターフェイス、または管理インターフェイスでは使用できません。

VLAN サブインターフェイスでの PTP フローは、適切な PTP 設定が親インターフェイス上に存在する場合にサポートされます。

PTPがどのモードでもイネーブルになっていない場合、このコマンドは受け入れられても何も効果がありません。警告が発行されます。

関連コマンド

コマンド	説明
show ptp clock	PTPクロックのプロパティを表示します。

ptp mode

ISA 3000 でPTP クロックモードを指定するには、特権EXEC モードまたはグローバル コンフィギュレーション モードで **ptp mode** コマンドを使用します。すべてのインターフェイスで PTP を無効にするには、このコマンドの **no** 形式を使用します。

ptp mode e2etransparent
no ptp mode

（注） このコマンドは、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

e2etranparent エンドツーエンド トランスペアレント モードを ISA 3000 上のすべての PTP 対応インターフェイスでイネーブルにします。

コマンド デフォルト

エンドツーエンド トランスペアレント モードはデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

エンドツーエンド トランスペアレント モードがディセーブルの場合、すべての PTP パケットは他のマルチキャスト パケットのように扱われます。これは転送モードと同等です。

ptp mode コマンドは、グローバル コンフィギュレーション モードでも使用できます。

例

次に、**ptp mode** コマンドを使用して、PTP クロックモードをエンドツーエンド トランスペアレントに設定する例を示します。

```
ciscoasa# ptp mode e2etranparent
```

関連コマンド

コマンド	説明
show ptp internal-info	PTP統計情報とカウンタ情報を表示します。

public-key

Cisco Umbrella によって要求される証明書の検証に DNSCrypt プロバイダーの公開キーを指定するには、Cisco Umbrella コンフィギュレーション モードで **public-key** コマンドを使用します。キーを削除して、デフォルトのキーを使用するには、このコマンドの **no** 形式を使用します。

public-key *dnscrypt_key*
no public-key [*dnscrypt_key*]

構文の説明

dnscrypt_key DNScrypt 用に Cisco Umbella サーバーによって使用される公開キー。このキーは、Cisco Umbrella のために使用される DNS インスペクション ポリシー マップで dnscrypt を有効にした場合にのみ関連します。

キーは 32 バイトの 16 進数値です。2 バイトごとにコロンで区切った ASCII の 16 進数値を入力します。キー長は 79 バイトです。このキーは Cisco Umbrella から取得します。

コマンド デフォルト

デフォルトのキーが使用されます。

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。

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

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

使用上のガイドライン

DNS インスペクション ポリシー マップで DNScrypt をイネーブルにする場合は、必要に応じて証明書の検証に DNScrypt プロバイダーの公開キーを設定できます。キーを設定しない場合は、現在配布されているデフォルトの公開キーが検証に使用されます。

キーの設定が必要になるのは、DNScrypt 暗号化に使用する公開キーが Cisco Umbrella によって変更された場合だけです。

例

次に、Cisco Umbrella で使用する公開キーを設定する例を示します。この例では、グローバル DNS インスペクションで使用されるデフォルトの DNS インスペクション ポリシー マップで DNScrypt を有効にする方法も示しています。

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

関連コマンド

コマンド	説明
dnscrypt	デバイスと Cisco Umbrella 間の接続で DNScrypt 暗号化を有効にします。
inspect dns	DNS インスペクションをイネーブルにします。
policy-map type inspect dns	DNS インスペクション ポリシー マップを作成します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバーからの応答がない場合、クライアントから Umbrella サーバーへの接続は削除されます。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

publish-crl

ローカル CA が発行した証明書の失効状態を他の ASA が検証できるようにするには、CA サーバー コンフィギュレーション モードで **publish-crl** コマンドを使用します。その結果、ASA のインターフェイスから CRL を直接ダウンロードできます。CRL をダウンロードできないようにするには、このコマンドの **no** 形式を使用します。

[**no**] **publish-crl interface** *interface* [**port** *portnumber*]

構文の説明

interface *interface*	インターフェイスに使用される *nameif* を指定します（gigabitethernet0/1 など）。詳細については、interface コマンドを参照してください。
port *portnumber*	（オプション）インターフェイス デバイスで CRL をダウンロードするときに使用するポートを指定します。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。

コマンド デフォルト

デフォルト **publish-crl** ステータスは **no publish** です。TCP ポート 80 は、HTTP のデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CRL は、デフォルトでアクセス不可です。必要なインターフェイスおよびポートで CRL ファイルへのアクセスをイネーブルにする必要があります。

TCP ポート 80 は、HTTP のデフォルト ポート番号です。デフォルト以外のポート（ポート 80 以外）を設定する場合は、他のデバイスがそのポートへのアクセス方法を認識できるように、**cdp-url** 構成にその新しいポート番号が含まれるようにします。

CRL 配布ポイント（CDP）は、ローカル CA ASA における CRL の場所です。**cdp-url** コマンドで設定する URL は、発行されるすべての証明書に埋め込まれます。CDP 用に特定の場所を設定しない場合、デフォルトの CDP の URL は http://hostname.domain/+CSCOCA+/asa_ca.crl です。

クライアントレスSSL VPNが同じインターフェイスでイネーブルになっている場合、HTTPリダイレクトとCRLダウンロード要求は、同じHTTPリスナーによって処理されます。リスナーが着信URLをチェックし、**cdp-url**コマンドで設定したURLと一致する場合、CRLファイルがダウンロードされます。URLが**cdp-url**コマンドと一致しない場合、接続がHTTPSにリダイレクトされます（HTTPリダイレクトが有効な場合）。

例

次に、CAサーバー コンフィギュレーション モードで**publish-crl**コマンドを入力して、外部インターフェイスのポート70をCRLダウンロード用に有効にする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa (config-ca-server)#publish-crl outside 70
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	自動生成されるCRL用に特定の場所を指定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

pwd

現在の作業ディレクトリを表示するには、特権 EXEC モードで **pwd** コマンドを使用します。

pwd

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ルート ディレクトリ（/）がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**dir** コマンドと機能が類似しています。

例

次に、現在の作業ディレクトリを表示する例を示します。

```
ciscoasa# pwd
disk0:/
ciscoasa# pwd
flash:
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
dir	ディレクトリの内容を表示します。
more	ファイルの内容を表示します。

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