



## tl ~ tz

---

- [tls-proxy](#) (3 ページ)
- [トークン](#) (5 ページ)
- [tos](#) (7 ページ)
- [traceroute](#) (9 ページ)
- [track rtr](#) (12 ページ)
- [traffic-forward](#) (14 ページ)
- [traffic-non-sip](#) (17 ページ)
- [transfer-encoding](#) (19 ページ)
- [trustpoint \(saml idp\)](#) (22 ページ)
- [trustpoint \(SSO サーバー\) \(非推奨\)](#) (24 ページ)
- [trust-verification-server](#) (26 ページ)
- [tsig enforced](#) (28 ページ)
- [ttl-evasion-protection](#) (30 ページ)
- [tunnel destination](#) (32 ページ)
- [トンネル モード](#) (34 ページ)
- [tunnel protection ipsec](#) (36 ページ)
- [tunnel source interface](#) (38 ページ)
- [tunnel-group](#) (40 ページ)
- [tunnel-group general-attributes](#) (43 ページ)
- [tunnel-group ipsec-attributes](#) (45 ページ)
- [tunnel-group-list enable](#) (47 ページ)
- [tunnel-group-map](#) (49 ページ)
- [tunnel-group-map default-group](#) (52 ページ)
- [tunnel-group-map enable](#) (54 ページ)
- [tunnel-group ppp-attributes](#) (56 ページ)
- [tunnel-group-preference](#) (58 ページ)
- [tunnel-group webvpn-attributes](#) (60 ページ)
- [tunnel-limit](#) (62 ページ)
- [tx-ring-limit](#) (64 ページ)

- [type echo](#) (67 ページ)

# tls-proxy

TLS コンフィギュレーション モードで TLS プロキシ インスタンスを設定したり、最大セッション数を設定したりするには、グローバル コンフィギュレーション モードで `tls-proxy` 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。

`tls-proxy` [ `maximum-sessions` *max\_sessions* / *proxy\_name* ] [ `noconfirm` ]  
`no tls-proxy` [ `maximum-sessions` *max\_sessions* / *proxy\_name* ] [ `noconfirm` ]

## 構文の説明

<i>max_sessions</i> <i>max_sessions</i>	プラットフォームでサポートする TLS プロキシ セッションの最大数を指定します。
<code>noconfirm</code>	確認を要求せずに <code>tls-proxy</code> コマンドを実行します。
<i>proxy_name</i>	TLS プロキシ インスタンスの名前を指定します。

## 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
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

## コマンド履歴

リリース 変更内容  
 ス

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-proxy` コマンドを使用して TLS プロキシ コンフィギュレーション モードを開始し、TLS プロキシ インスタンスを作成したり、プラットフォームでサポートされる最大セッション数を設定したりできます。

## 例

次の例では、TLS プロキシ インスタンスを作成する方法を示します。

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client ldc issuer ldc_server
ciscoasa(config-tlsp)# client ldc keypair phone_common
```

## 関連コマンド

コマンド	説明
<b>client</b>	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
<b>ctl-provider</b>	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。
<b>server trust-point</b>	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。
<b>show tls-proxy</b>	TLS プロキシを表示します。

# トークン

Cisco Umbrella に登録するために必要な API トークンを設定するには、Umbrella コンフィギュレーション モードで **token** コマンドを使用します。トークンを削除するには、このコマンドの **no** 形式を使用します。

**token** *api-token*  
**no token** *api-token*

## 構文の説明

*api-token* Cisco Umbrella への登録に必要な API トークン。Cisco Umbrella ネットワーク デバイス ダッシュ ボード (<https://login.umbrella.com/>) からトークンを取得する必要があります。トークンは、16 進数の文字列、たとえば、AABBA59A0BDE1485C912AFE になります。

## コマンドデフォルト

デフォルトの API トークンはありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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 変更内容  
 ス

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

Cisco Umbrella にデバイスを正常に登録するには、API トークンを設定する必要があります。トークンは顧客ごとに一意であり、デバイスごとに一意ではありません。

登録は、スタンドアロン デバイス、クラスタ、またはフェールオーバー グループに対して行われます。クラスタまたはフェールオーバー グループ内の各デバイスを個別に登録はしません。マルチ コンテキスト モードでは、各コンテキストは、スタンドアロンか、クラスタまたはフェールオーバー グループ内に存在するかに関わらず、デバイスです。

## 例

次の例では、API トークンを Cisco Umbrella に登録するよう設定します。

```
ciscoasa(config)# umbrella-global
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

#### 関連コマンド

コマンド	説明
<b>public-key</b>	Cisco Umbrella で使用する公開キーを設定します。
<b>timeout edns</b>	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。
<b>umbrella-global</b>	Cisco Umbrella グローバルパラメータを設定します。

## tos

SLA 動作要求パケットの IP ヘッダー内のタイプオブサービスバイトを定義するには、SLA モニタープロトコルコンフィギュレーションモードで **tos** 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。

**tos number**

**no tos**

### 構文の説明

*number* IPヘッダーで使用するサービスタイプの値。有効な値は、0～255です。

### コマンドデフォルト

デフォルトのタイプオブサービス値は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
SLA モニター プロトコル コンフィギュ レーション	• 対応	—	• 対応	—	—

### コマンド履歴

リリース 変更内容  
ス

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

このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。これは、専用アクセスレートなどのポリシールーティングおよび機能のために、ネットワーク上の他のルータによって使用されます。

### 例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。エコー要求パケットのペイロードサイズを 48 バイトに設定し、SLA 動作中に送信されるエコー要求数を 5 に、さらにタイプオブサービスバイトを 80 に設定します。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# tos 80
```

```

ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability

```

---

**関連コマンド**

コマンド	説明
<b>num-packets</b>	SLA 動作中に送信する要求パケットの数を指定します。
<b>request-data-size</b>	要求パケットのペイロードのサイズを指定します。
<b>sla monitor</b>	SLA モニタリング動作を定義します。
<b>type echo</b>	SLA 動作をエコー応答時間プローブ動作として設定します。



# traceroute

パケットが宛先に到達するまでのルートを特定するには、**traceroute** コマンドを使用します。

```
traceroute destination_ip / hostname [ source source_ip / source-interface ] [ numeric ] [ timeout timeout_value ] [ probe probe_num ] [ ttl min_ttl max_ttl ] [ port port_value ] [ use-icmp ]
```

## 構文の説明

<i>destination_ip</i>	<b>traceroute</b> の宛先 IP アドレスを指定します。IPv4 アドレスと IPv6 アドレスの両方をサポートします。
<i>hostname</i>	ルートをトレースする先のホストのホスト名。ホストの宛先には、IPv4 または IPv6 アドレスを使用できます。ホスト名を指定する場合は、 <b>name</b> コマンドで定義するか、 <b>traceroute</b> をイネーブルにしてホスト名を IP アドレスに解決するように DNS サーバーを設定します。www.example.com などの DNS ドメイン名をサポートします。
<i>max-ttl</i>	使用可能な最大 TTL 値。デフォルトは 30 です。 <b>traceroute</b> パケットが宛先に到達するか、値に達したときにコマンドは終了します。
<i>min_ttl</i>	最初のプローブの TTL 値。デフォルトは 1 ですが、既知のホップの表示を抑制するためにより大きい値を設定できます。
<b>numeric</b>	出力に中間ゲートウェイの IP アドレスのみが示されるように指定します。このキーワードを指定しない場合は、トレース中に到達したゲートウェイのホスト名の検索を試みます。
<b>port</b> <i>port_value</i>	ユーザーデータグラムプロトコル (UDP) プローブメッセージによって使用される宛先ポート。デフォルトは 33434 です。
<b>probe</b> <i>probe_num</i>	TTL の各レベルで送信するプローブの数。デフォルト数は 3 です。
<b>source</b>	トレースパケットの送信元として使用される IP アドレスまたはインターフェイスを指定します。IPv6 では、IPv6 送信元アドレスのみが受け入れられます。
<i>source_interface</i>	パケットトレースの送信元インターフェイスを指定します。指定する場合は、送信元インターフェイスの IP アドレスが使用されます。
<i>source_ip</i>	パケットトレースの送信元 IP アドレスを指定します。この IP アドレスはいずれかのインターフェイスの IP アドレスにする必要があります。トランスペアレントモードの場合は、ASA の管理 IP アドレスにする必要があります。
<b>timeout</b>	使用されるタイムアウト値を指定します。
<i>timeout_value</i>	接続をタイムアウトにする前に応答を待機する時間を指定します。デフォルトは 3 秒です。

<b>ttl</b>	プローブで使用する存続可能時間の値の範囲を指定するキーワード。
<b>use-icmp</b>	UDP プローブ パケットの代わりに ICMP プローブ パケットを使用するように指定します。

**コマンド デフォルト** このコマンドには、デフォルト設定がありません。

**コマンド モード** 次の表に、コマンドを入力できるモードを示します。

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

**コマンド履歴**

リリース 変更内容  
ス

7.2(1) このコマンドが追加されました。

9.7(1) このコマンドは、IPv6 アドレスを受け入れるように更新されました。

**使用上のガイドライン**

**tracert** コマンドは、送信した各プローブの結果を出力します。出力の各行が 1 つの TTL 値に対応します（昇順）。次に、**tracert** コマンドによって表示される出力記号を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
U	宛先へのルートが存在しません。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。ICMPv6 では、アドレスは対象外です。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。ICMPv6 では、ポートが到達不能です。
!A	ICMP が管理者によって禁止されています。
?	原因不明の ICMP エラーが発生しました。

例

次に、宛先 IP アドレスを指定した場合の **tracert** 出力の例を示します。

```

ciscoasa# traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1 10.83.194.1 0 msec 10 msec 0 msec
 2 10.83.193.65 0 msec 0 msec 0 msec
 3 10.88.193.101 0 msec 10 msec 0 msec
 4 10.88.193.97 0 msec 0 msec 10 msec
 5 10.88.239.9 0 msec 10 msec 0 msec
 6 10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
ciscoasa/admin(config)# traceroute 2002::130
Type escape sequence to abort.
Tracing the route to 2002::130
 1 5000::2 0 msec 0 msec 0 msec
 2 2002::130 10 msec 0 msec 0 msec

```

---

**関連コマンド**

コマンド	説明
<b>capture</b>	トレース パケットを含めて、パケット情報をキャプチャします。
<b>show capture</b>	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。
<b>packet-tracer</b>	パケット トレース機能をイネーブルにします。

## track rtr

SLA 動作の到達可能性を追跡するには、グローバル コンフィギュレーション モードで **track rtr** コマンドを使用します。SLA 追跡を削除するには、このコマンドの **no** 形式を使用します。

**track track-id rtr sla-id reachability**  
**no track track-id rtr sla-id reachability**

### 構文の説明

**reachability** オブジェクトの到達可能性を追跡するように指定します。

**sla-id**      トラッキング エントリが使用する SLA の ID。

**track-id**    トラッキング エントリ オブジェクト ID を作成します。有効な値は、1 ~ 500 です。

### コマンド デフォルト

SLA 追跡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 コンフィギュレーション	• 対応	—	• 対応	—	—

### コマンド履歴

リリー    変更内容  
 ス

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

**track rtr** コマンドは、トラッキング エントリ オブジェクト ID を作成し、トラッキング エントリが使用する SLA を指定します。

各 SLA 動作が、トラッキング プロセスによって解釈される動作戻りコード値を維持します。戻りコードには、OK や Over Threshold などのいくつかの戻りコードがあります。表 2-1 に、これらの戻りコードに関連するオブジェクトの到達可能性ステータスを示します。

表 1: SLA 追跡の戻りコード

トラッキング	戻りコード	追跡ステータス
到達可能性	OK または Over Threshold	Up
	他の任意のコード	Down

## 例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

## 関連コマンド

コマンド	説明
<b>route</b>	スタティック ルートを設定します。
<b>sla monitor</b>	SLA モニタリング動作を定義します。

## traffic-forward

トラフィックをモジュールに転送し、アクセス制御とその他の処理をバイパスするには、インターフェイス コンフィギュレーション モードで **traffic-forward** コマンドを使用します。トラフィック転送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。

**traffic-forward module\_type monitor-only**  
**no traffic-forward module\_type monitor-only**

### 構文の説明

*module\_type* モジュールのタイプサポートされるモジュールは次のとおりです。

- **sfr** : ASA FirePOWER モジュール。
- **cxsc** : ASA CX モジュール。

**monitor-only** モジュールをモニター専用モードに設定します。モニター専用モードでは、モジュールはトラフィックを処理できますが、その後トラフィックをドロップします。モジュールタイプによって使用方法は異なります。

- **ASA FirePOWER** : このコマンドを使用して、パッシブ モードを設定します。このモードは実稼働用に使用できます。
- **ASA CX** : これは厳密にはデモンストレーションモードです。トラフィック転送インターフェイスまたはデバイスを実稼働用に使用することはできません。

### 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  
 ス

9.1(2) このコマンドが追加されました。

---

**リリース**    **変更内容**


---

9.2(1)    **sfr** キーワードが追加されました。

---

9.3(2)    **sfr** キーワードの実稼働での使用のサポートが追加されました。

---



---

**使用上のガイドライン**

**monitor-only** キーワードを指定してサービスポリシーの **sfr** または **cxsc** コマンドを使用する代わりに、このコマンドでトラフィックをモジュールにリダイレクトできます。サービスポリシーにより、トラフィックは依然として、廃棄トラフィックを生じる可能性があるアクセスルールやTCP正規化などのASAの処理が前提となっています。さらに、ASAはトラフィックのコピーを単純にモジュールに送信して、最終的にはそれ自身のポリシーに従ってトラフィックを送信します。

一方で、**traffic-forward** コマンドはASA処理を完全にバイパスして、トラフィックを単純にモジュールに転送します。モジュールは、トラフィックを検査し、ポリシーを決定し、イベントを生成して、インラインモードで動作した場合に、トラフィックに対してどのような処理が行われることになるかを示します。モジュールはトラフィックのコピーに対して動作しますが、ASA自体は、ASAまたはモジュールのポリシー決定に関係なくトラフィックを即座にドロップします。モジュールは、ブラックホールの役割を果たします。

トラフィック転送インターフェイスをネットワーク内のスイッチのSPANポートに接続します。

トラフィック転送インターフェイス コンフィギュレーションには次の制限があります。

- ASA上でモニター専用モードと通常のインラインモードの両方を同時に設定することはできません。セキュリティポリシーの1つのタイプのみが許可されます。
- ASAはシングルコンテキストトランスペアレントモードである必要があります。
- トラフィック転送インターフェイスは、VLANまたはBVIではなく、物理インターフェイスである必要があります。また、物理インターフェイスには、それに関連付けられたVLANを設定することはできません。
- トラフィック転送インターフェイスは、ASAトラフィックには使用できません。これらに名前を付けたり、フェールオーバーや管理専用を含むASA機能向けに設定したりすることはできません。

---

**例**

次の例は、GigabitEthernet0/5をトラフィック転送インターフェイスとして設定します。

```
interface gigabitethernet 0/5
no nameif
traffic-forward sfr monitor-only
no shutdown
```

## 関連コマンド

コマンド	説明
<b>interface</b>	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。
<b>cxsc</b>	トラフィックを ASA CX モジュールにリダイレクトするサービス ポリシー コマンド。
<b>sfr</b>	トラフィックを ASA FirePOWER モジュールにリダイレクトするサービスポリシーコマンド。



## traffic-non-sip

既知の SIP シグナリングポートを使用する非 SIP トラフィックを許可するには、パラメータ コンフィギュレーション モードで **traffic-non-sip** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**traffic-non-sip**  
**no traffic-non-sip**

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

9.16以降、このコマンドはデフォルトでディセーブルになっています。以前のリリースでは、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
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。

9.16(1) デフォルト設定がディセーブルに変更されました。

### 例

次に、SIP インспекション ポリシー マップで既知の SIP シグナリング ポートを使用する非 SIP トラフィックを許可する例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# traffic-non-sip
```

### 関連コマンド

コマンド	説明
<b>class</b>	ポリシー マップのクラス マップ名を指定します。

コマンド	説明
<b>class-map type inspect</b>	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。
<b>policy-map</b>	レイヤ 3/4 のポリシー マップを作成します。
<b>show running-config policy-map</b>	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。

## transfer-encoding

転送エンコーディングタイプを指定してHTTPトラフィックを制限するには、**http-map** コマンドを使用してアクセス可能なHTTPマップコンフィギュレーションモードで、**transfer-encoding** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

```
transfer-encoding type { chunked | compress | deflate | gzip | identity | default } action { allow |
reset | drop } [ log ]
no transfer-encoding type { chunked | compress | deflate | gzip | identity | default } action { allow |
reset | drop } [ log ]
```

### 構文の説明

<b>action</b>	指定した転送エンコーディングタイプを使用する接続が検出されたときに実行するアクションを指定します。
<b>allow</b>	メッセージを許可します。
<b>chunked</b>	メッセージ本文を一連のチャンクとして転送する転送エンコーディングタイプを識別します。
<b>compress</b>	メッセージ本文をUNIXファイル圧縮を使用して転送する転送エンコーディングタイプを識別します。
<b>default</b>	トラフィックが、設定されたリストにないサポートされる要求方式を含む場合にASAが実行するデフォルトのアクションを指定します。
<b>deflate</b>	メッセージ本文をzlib形式(RFC 1950)とデフレート圧縮(RFC 1951)を使用して転送する転送エンコーディングタイプを識別します。
<b>drop</b>	接続を閉じます。
<b>gzip</b>	メッセージ本文をGNU zip(RFC 1952)を使用して転送する転送エンコーディングタイプを識別します。
<b>identity</b>	転送エンコーディングが実行されていないメッセージ本文の接続を識別します。
<b>log</b>	(任意) syslogを生成します。
<b>reset</b>	TCPリセットメッセージをクライアントおよびサーバーに送信します。
<b>type</b>	HTTPアプリケーションインスペクションを通じて制御される転送エンコーディングのタイプを指定します。

### コマンドデフォルト

このコマンドは、デフォルトでディセーブルになっています。コマンドがイネーブルで、サポートされる転送エンコーディングタイプが指定されていない場合、デフォルトアクションでは、ロギングなしで接続を許可します。デフォルトのアクションを変更するには、**default** キーワードを使用して、別のデフォルトアクションを指定します。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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
HTTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

## コマンド履歴

リリース 変更内容  
ス

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

**transfer-encoding** コマンドがイネーブルの場合、ASA は、サポートされ設定されている各転送エンコーディングタイプの HTTP 接続に指定されたアクションを適用します。

ASA は、設定されたリストの転送エンコーディングタイプに一致しないすべてのトラフィックに **default** のアクションを適用します。設定済みの **default** のアクションでは、ロギングなしで接続を **allow** します。

たとえば、設定済みのデフォルトのアクションでは、**drop** と **log** のアクションを伴う 1 つ以上のエンコーディングタイプを指定した場合、ASA は、設定されたエンコーディングタイプを含む接続をドロップし、各接続をロギングし、その他のサポートされるエンコーディングタイプの接続をすべて許可します。

より限定的なポリシーを設定する場合は、デフォルトのアクションを **drop**（または **reset**）と **log**（イベントをロギングする場合）に変更します。その後、許可されたエンコーディングタイプのそれぞれに **allow** アクションを設定します。

**transfer-encoding** コマンドは、適用する設定ごとに 1 回ずつ入力します。デフォルトアクションを変更するために **transfer-encoding** コマンドの 1 つのインスタンスを使用し、設定された転送エンコーディングタイプのリストに各エンコーディングタイプを追加するために 1 つのインスタンスを使用します。

設定されたアプリケーションタイプのリストからアプリケーションカテゴリを削除するために、このコマンドの **no** 形式を使用する場合は、コマンドラインのアプリケーションカテゴリキーワードの後ろの文字はすべて無視されます。

## 例

次に、特に禁止されていないすべてのサポートされるアプリケーションタイプを許可する設定済みのデフォルトを使用して、許可ポリシーを提供する例を示します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# transfer-encoding gzip drop log
ciscoasa(config-http-map)#
```

この場合、GNU zip を使用する接続だけがドロップされ、そのイベントがロギングされます。

次に、デフォルトアクションを、接続のリセットと、特に許可されていないすべてのエンコーディングタイプのロギングに変更した、限定的なポリシーを提供する例を示します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# port-misuse default action reset log
ciscoasa(config-http-map)# port-misuse identity allow
ciscoasa(config-http-map)#
```

この場合、転送エンコーディングを使用していない接続だけが許可されます。他のサポートされるエンコーディングタイプの HTTP トラフィックを受信した場合は、ASA は接続をリセットして syslog エントリを作成します。

#### 関連コマンド

コマンド	説明
<b>class-map</b>	セキュリティアクションを適用するトラフィック クラスを定義します。
<b>debug appfw</b>	拡張 HTTP インспекションに関連するトラフィックの詳細情報を表示します。
<b>http-map</b>	拡張 HTTP インспекションを設定するための HTTP マップを定義します。
<b>inspect http</b>	アプリケーション インспекション用に特定の HTTP マップを適用します。
<b>policy-map</b>	特定のセキュリティアクションにクラス マップを関連付けます。

## trustpoint (saml idp)

IDP 認証または SP 認証の証明書を含むトラストポイントを設定するには、SAML IDP コンフィギュレーションモードで **trustpoint** コマンドを使用します。SAML IDP 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 **webvpn** コマンドを入力します。トラストポイントを削除するには、このコマンドの **no** 形式を使用します。

```
trustpoint { idp | sp } trustpoint-name
no trustpoint { idp | sp } trustpoint-name
```

### 構文の説明

*trustpoint-name* 使用するトラストポイントの名前を指定します。

**sp**                    トラストポイントには、ASA の署名を確認したり SAML アサーションを暗号化するための IdP の ASA (SP) 証明書が含まれます。

**idp**                    トラストポイントには、SAML アサーションを確認するための ASA の IdP 証明書が含まれます。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
SAML IDP コンフィギュレーション	• 対応	—	• 対応	—	—

### コマンド履歴

リリー    変更内容  
ス

9.5(2)    このコマンドが追加されました。

### 使用上のガイドライン

トラストポイントは、特に認証パスの最初の公開キーを提供するために使用される公開キー証明書をはじめ、検証テストの必要なく有効であることを信頼できる CA 発行の証明書に基づいて、認証局 ID を表します。

## 関連コマンド

コマンド	説明
saml idp	サードパーティ製 IdP の設定を作成し、SAML 属性を設定できるように SAML IDP モードを開始します。

## trustpoint (SSO サーバー) (非推奨)



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

SAML POST-type SSO サーバーに送信される証明書を識別するトラストポイントの名前を指定するには、SSO サーバーモードで **trustpoint** コマンドを使用します。トラストポイン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。

**trustpoint** *trustpoint-name*  
**no trustpoint** *trustpoint-name*

### 構文の説明

*trustpoint-name* 使用するトラストポイントの名前を指定します。

### 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
<b>config webvpn sso saml</b>	• 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す。

9.5(2) SAML 2.0 がサポートされたため、このコマンドは廃止されました。

### 使用上のガイドライン

シングルサインオンは、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスにアクセスできます。ASA は現在、SAML POST-type の SSO サーバーと SiteMinder-type の SSO サーバーをサポートしています。

このコマンドは、SAML-type の SSO サーバーのみに適用されます。

トラストポイントは、特に認証パスの最初の公開キーを提供するために使用される公開キー証明書をはじめ、検証テストの必要なく有効であることを信頼できる CA 発行の証明書に基づいて、認証局 ID を表します。



## 例

次に、config-webvpn-sso-saml モードを開始し、SAML POST-type SSO サーバーに送信される証明書を識別するトラストポイントに名前を付ける例を示します。

```
ciscoasa(config-webvpn)# sso server
ciscoasa(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

## 関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント情報を管理します。
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 サーバーの運用統計情報を表示します。
sso server	SSO サーバーのタイプを作成、命名、および指定します。

## trust-verification-server

HTTPS の確立時に Cisco Unified IP Phones でのアプリケーションサーバーの認証を可能にする信頼検証サービスサーバーを指定するには、SIP インспекションのパラメータコンフィギュレーションモードで **trust-verification-server** コマンドを使用します。パラメータコンフィギュレーションモードには、ポリシーマップコンフィギュレーションモードからアクセスできません。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。

```
trust-verification-server { ip address | port number }
no trust-verification-server { ip address | port number }
```

### 構文の説明

**ip address** 信頼検証サービスサーバーの IP アドレスを指定します。SIP インспекションポリシーマップでこの引数を指定してこのコマンドを入力できるのは 4 回までです。SIP インспекションは、登録された電話機ごとに各サーバーへのピンホールを開き、電話機はどのサーバーを使用するかを決定します。Cisco Unified Communications Manager (CUCM) サーバーで、信頼検証サービスサーバーを設定します。

**port number** サーバーが使用するポート番号を指定します。使用できるポート範囲は 1026 ~ 32768 です。

### コマンド デフォルト

デフォルトポートは 2445 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
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 変更内容  
ス

9.3(2) このコマンドが追加されました。

### 例

次に、SIP インспекションポリシーマップで 4 つの信頼検証サービスサーバーを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
```

```
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.1
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.2
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.3
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.4
ciscoasa(config-pmap-p)# trust-verification-server port 2445
```

## 関連コマンド

コマンド	説明
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>show running-config policy-map</b>	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。

## tsig enforced

TSIG リソースレコードの存在を必須とするには、パラメータ コンフィギュレーション モードで **tsig enforced** 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。

```
tsig enforced action { drop [ log ] | log }
no tsig enforced [ action { drop [ log ] | log }]
```

### 構文の説明

**drop** TSIG が存在しない場合にパケットをドロップします。

**log** システム メッセージ ログを生成します。

### コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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 変更内容  
ス

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、DNS トランザクションにおける TSIG の存在のモニターと強制をイネーブルにします。

### 例

次に、DNS インспекション ポリシー マップ内で TSIG 強制をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tsig enforced action log
```

## 関連コマンド

コマンド	説明
<b>class</b>	ポリシー マップのクラス マップ名を指定します。
<b>class-map type inspect</b>	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。
<b>policy-map</b>	レイヤ 3/4 のポリシー マップを作成します。
<b>show running-config policy-map</b>	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。

## ttl-evasion-protection

存続可能時間（TTL）回避保護をイネーブルにするには、TCP マップ コンフィギュレーション モードで **ttl-evasion-protection** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

**ttl-evasion-protection**  
**no ttl-evasion-protection**

### 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

提供される TTL 回避保護は、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
TCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

### コマンド履歴

リリー 変更内容  
ス

7.0(1) このコマンドが追加されました。

### 使用上のガイドライン

**tcp-map** コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

**tcp-map** コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。TCP マップ コンフィギュレーション モードで **ttl-evasion-protection** コマンドを使用して、セキュリティポリシーを回避しようとする攻撃を阻止できます。TTL 回避保護により、接続の最大 TTL は最初のパケットの TTL によって決定します。後続パケットの TTL は削減できますが、増やすことはできません。システムは、TTL をその接続の以前の最小 TTL にリセットします。

たとえば、攻撃者は非常に短い TTL を持ち、ポリシーに合致するパケットを送信できます。TTL がゼロになると、ASA とエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、ASA にとって再送信のように見えるため、通過します。一方、エンドポイントホストにとっ

では、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。この機能をイネーブルにすると、このような攻撃を阻止します。

## 例

次に、ネットワーク 10.0.0.0 から 20.0.0.0 へのフローに対して TTL 回避保護をディセーブルにする例を示します。

```
ciscoasa(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# no
ttl-evasion-protection
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP1
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

## 関連コマンド

コマンド	説明
<b>class</b>	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。
<b>policy-map</b>	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。
<b>set connection</b>	接続値を設定します。
<b>tcp-map</b>	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

## tunnel destination

VTI トンネルの宛先の IP アドレス (IPv4 または IPv6) 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 **tunnel destination** コマンドを使用します。VTI トンネルの宛先 IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
tunnel destination { IP address / hostname }
no tunnel destination { IP address / hostname }
```

### 構文の説明

*IPアドレス* VTI トンネルの宛先の IP アドレス (IPv4 または IPv6) を指定します。

*hostname* VTI トンネルの宛先のホスト名を指定します。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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  
ス

9.7(1) このコマンドが追加されました。

9.16(1) IPv6 アドレスのサポートが導入されました。

### 使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用した後、インターフェイス コンフィギュレーション モードで使用できます。

### 例

次の例では、VTI トンネルの宛先の IP アドレスを指定します。

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel destination 10.2.2.3
```



## 関連コマンド

コマンド	説明
<b>interface tunnel</b>	新しい VTI トンネル インターフェイスを作成します。
<b>tunnel source interface</b>	VTI トンネルを作成するための送信元インターフェイスを指定します。
<b>tunnel mode</b>	IPsec がトンネル保護に使用されることを指定します。
<b>tunnel protection ipsec</b>	トンネル保護に使用される IPsec プロファイルを指定します。

# トンネルモード

VTIトンネルにトンネル保護モードを指定するには、**tunnel mode** コマンドをインターフェイスコンフィギュレーションモードで使用します。トンネルでは、IPSec over IPv4 または IPv6 を使用できます。VTI トンネル保護を削除するには、このコマンドの **no** 形式を使用します。

```
tunnel mode ipsec { ipv4 | ipv6 }
no tunnel mode ipsec { ipv4 | ipv6 }
```

## 構文の説明

**ipsec** トンネル保護基準としてトンネルがIPsecを使用することを指定します。

**ipv4** トンネルがIPsec over IPv4を使用することを指定します。

**ipv6** トンネルがIPsec over IPv6を使用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

次の表は、このコマンドを入力できるモードを示しています。

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 変更内容  
ス

9.7(1) このコマンドが追加されました。

9.16(1) IPSec over IPv6 を導入しました。

## 使用上のガイドライン

このコマンドは、グローバルコンフィギュレーションモードで **interface tunnel** コマンドを使用した後、インターフェイスコンフィギュレーションモードで使用できます。

## 例

次の例では、保護モードとしてIPsecを指定します。

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel mode ipsec ipv4
```

## 関連コマンド

コマンド	説明
<b>interface tunnel</b>	新しい VTI トンネル インターフェイスを作成します。
<b>tunnel source interface</b>	VTI トンネルを作成するための送信元インターフェイスを指定します。
<b>tunnel destination</b>	VTI トンネルの宛先の IP アドレスを指定します。
<b>tunnel protection ipsec</b>	トンネル保護に使用される IPsec プロファイルを指定します。

## tunnel protection ipsec

VTI トンネルに IPsec プロファイルを指定するには、`tunnel protection ipsec` コマンドをインターフェイス コンフィギュレーション モードで使用します。トンネルから IPsec プロファイルを削除するには、このコマンドの `no` 形式を使用します。

**tunnel protection ipsec** *IPsec profile name*  
**no tunnel protection ipsec** *IPsec profile name*

### 構文の説明

*ipsec profile name* 使用する IPsec プロファイルの名前を指定します。

### 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

次の表は、このコマンドを入力できるモードを示しています。

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  
 ス

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

このコマンドは、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用した後、インターフェイス コンフィギュレーション モードで使用できます。このコマンドを使用すると、IKEv1 ポリシーが IPsec プロファイルに接続されます。

### 例

次の例では、`profile12` が IPsec プロファイルです。

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel protection ipsec profile12
```

### 関連コマンド

コマンド	説明
<b>interface tunnel</b>	新しい VTI トンネル インターフェイスを作成します。

コマンド	説明
<b>tunnel source interface</b>	VTI トンネルを作成するための送信元インターフェイスを指定します。
<b>tunnel destination</b>	VTI トンネルの宛先の IP アドレスを指定します。
<b>tunnel mode</b>	IPsec がトンネル保護に使用されることを指定します。

## tunnel source interface

VTI トンネルに送信元インターフェイスを指定するには、`tunnel source interface` コマンドをインターフェイスコンフィギュレーションモードで使用します。VTI トンネルの送信元インターフェイスを削除するには、このコマンドの `no` 形式を使用します。

```
tunnel source interface interface_name
tunnel source interface interface_name ipv6 ipv6_address
no tunnel source interface interface_name
no tunnel source interface interface_name ipv6 ipv6_address
```

### 構文の説明

`interface_name` VTI トンネルを作成するために使用される送信元インターフェイスを指定します。送信元インターフェイスが IPv6 アドレスの場合は、そのアドレスの前に `ipv6` を付けます。

### 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

次の表は、このコマンドを入力できるモードを示しています。

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  
ス

9.7(1) このコマンドが追加されました。

9.16(1) IPv6 アドレスのサポートが導入されました。

### 使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードで `interface tunnel` コマンドを使用した後、インターフェイスコンフィギュレーションモードで使用できます。IP アドレスは、選択されたインターフェイスから取得されます。

### 例

次の例では、VTI トンネルの送信元インターフェイスを指定します。

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel source interface outside
```

## 関連コマンド

コマンド	説明
<b>interface tunnel</b>	新しい VTI トンネル インターフェイスを作成します。
<b>tunnel destination</b>	VTI トンネルの宛先の IP アドレスを指定します。
<b>tunnel mode</b>	IPsec がトンネル保護に使用されることを指定します。
<b>tunnel protection ipsec</b>	トンネル保護に使用される IPsec プロファイルを指定します。

# 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し管理するには、グローバル コンフィギュレーション モードで **tunnel-group** コマンドを使用します。トンネルグループを削除するには、このコマンドの **no** 形式を使用します。

**tunnel-group** *name* *type* *type*  
**no tunnel-group** *name*

## 構文の説明

*name* トンネル グループの名前を指定します。任意のストリングを選択できます。名前が IP アドレスの場合は、通常、ピアの IP アドレスとなります。

*type* トンネル グループのタイプを指定します。

- **remote-access** : ユーザーに IPsec リモート アクセスまたは WebVPN (ポータルまたはトンネルクライアント) のいずれかを使用した接続を許可します。
- **ipsec-l2l** : 2つのサイトまたは LAN がインターネットなどのパブリック ネットワークを介してセキュアに接続できる IPsec LAN-to-LAN を指定します。

(注) 次のトンネルグループタイプはリリース 8.0(2) で廃止されました。 **ipsec-ra** : IPsec リモートアクセス、 **webvpn** : WebVPN。ASA はこれらを **remote-access** タイプに変換します。

## 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
グローバル コンフィギュレーション	• 対応	「注」を参照してください。	• 対応	• 対応	—



(注) **tunnel-group** コマンドは、トランスペアレントファイアウォールモードで使用可能です。このモードでは、LAN-to-LAN トンネル グループのコンフィギュレーションは設定できますが、**remote-access** グループまたは WebVPN グループの設定はできません。LAN-to-LAN に対応する **tunnel-group** コマンドはすべてトランスペアレントファイアウォールモードで使用できます。



コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが追加されました。
	7.1(1)	webvpn タイプが追加されました。
	8.0(2)	remote-access タイプが追加され、ipsec-ra タイプと webvpn タイプが廃止されました。
	8.3(1)	<i>name</i> 引数は、IPv6 アドレスに対応するために変更されました。
	9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
	9.15(1)	external-browser オプションは、config-tunnel-webvpn モードでは廃止されました。
	9.17(1)	AnyConnect 外部ブラウザを使用した WebAuthN サポートが追加されました。config-tunnel-webvpn モードに external-browser オプションが追加されています。

**使用上のガイドライン** SSL VPN ユーザー（AnyConnect およびクライアントレスの両方）は、次の各種方式を使用して、アクセスするトンネル グループを選択できます。

- group-url
- group-alias
- 証明書マップ（証明書を使用する場合）

このコマンドとサブコマンドによって、ユーザーが webvpn サービスにログインするときにドロップダウンメニューでグループを選択できるように ASA を設定します。メニューに表示されるグループは、ASA で設定された実際の接続プロファイル（トンネルグループ）のエイリアスまたは URL です。

ASA には、次のデフォルトトンネルグループがあります。

- DefaultRAGroup、デフォルトの IPsec remote-access トンネルグループ
- DefaultL2LGroup、デフォルトの IPsec LAN-to-LAN トンネルグループ
- DefaultWEBVPNGroup、デフォルトの WebVPN トンネルグループ

これらのグループは変更できますが、削除はできません。トンネルネゴシエーションで識別された特定のトンネルグループがない場合は、ASA は、これらのグループを使用して、リモートアクセスおよび LAN-to-LAN トンネルグループのデフォルトトンネルパラメータを設定します。

**tunnel-group** コマンドを入力した後、適切な後続のコマンドを入力して、特定のトンネルグループの特定の属性を設定できます。これらのコマンドはそれぞれ、トンネルグループ属性を設定するためのコンフィギュレーションモードを開始します。

- **tunnel-group general-attributes**

- tunnel-group ipsec-attributes
- tunnel-group webvpn-attributes
- tunnel-group ppp-attributes

LAN-to-LAN 接続の場合、ASA は、クリプトマップで設定されたピアアドレスを同名のトンネルグループと一致させることで、接続のためのトンネルグループを選択しようとします。そのため、IPv6 ピアに対し、その IPv6 のアドレスと同様にトンネルグループ名を設定する必要があります。トンネルグループ名は、短い表記または長い表記で設定できます。CLI を使うと、その名前を最短の表記にできます。たとえば、トンネルグループ コマンドを次のように入力した場合、

```
ciscoasa(config)# tunnel-group 2001:0db8:0000:0000:0000:0000:1428:57ab type ipsec-121
トンネルグループはコンフィギュレーションで次のように表示されます。
```

```
tunnel-group 2001:0db8::1428:57ab type ipsec-121
```

## 例

次に、グローバルコンフィギュレーションモードを開始する例を示します。最初に、リモートアクセス トンネルグループを設定します。グループ名は group1 です。

```
ciscoasa(config)# tunnel-group group1 type remote-access
ciscoasa(config)#
```

次に、webvpn トンネルグループ「group1」を設定する tunnel-group コマンドの例を示します。この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入力します。

```
ciscoasa(config)# tunnel-group group1 type webvpn
ciscoasa(config)#
```

## 関連コマンド

コマンド	説明
<b>clear configure tunnel-group</b>	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。
<b>show running-config tunnel-group</b>	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。
<b>tunnel-group general-attributes</b>	設定一般モードを開始し、全般的なトンネルグループ属性を設定します。
tunnel-group ipsec-attributes	設定 ipsec モードを開始し、IPsec トンネルグループ属性を設定します。
tunnel-group ppp-attributes	L2TP 接続の PPP 設定を行うための設定 ppp モードを開始します。
tunnel-group webvpn-attributes	WebVPN トンネルグループ属性を設定する設定 webvpn モードを開始します。

## tunnel-group general-attributes

一般属性コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **tunnel-group general-attributes** コマンドを使用します。このモードは、すべてのサポートされるトンネリングプロトコルに共通の設定値を設定するために使用されます。

すべての一般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。

**tunnel-group name general-attributes**  
**no tunnel-group name general-attributes**

### 構文の説明

**general-attributes** このトンネルグループの属性を指定します。

**name** トンネルグループの名前を指定します。

### 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
トンネルグループ一般属性コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

### コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

7.1(1) 他のトンネルグループタイプのさまざまな属性が、一般トンネルグループ属性リストに移行され、トンネルグループ一般属性モードのプロンプトが変更されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

### 例

次に、グローバルコンフィギュレーションモードを開始し、LAN-to-LAN ピアの IP アドレスを使用してリモートアクセス接続のリモートアクセストンネルグループを作成し、その後、トンネルグループ一般属性を設定するための一般属性コンフィギュ

レーションモードを開始する例を示します。トンネルグループの名前は、209.165.200.225 です。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type remote-access
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
ciscoasa(config-tunnel-general)#
```

次に、グローバル コンフィギュレーション モードで、IPsec リモート アクセス接続用のトンネルグループ「remotegrp」を作成し、その後、トンネルグループ「remotegrp」の一般属性を設定するための一般コンフィギュレーションモードを開始する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)
```

#### 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。

## tunnel-group ipsec-attributes

IPSec 属性コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **tunnel-group ipsec-attributes** コマンドを使用します。このモードは、IPsec トンネリングプロトコルに固有の設定値を設定するために使用されます。

すべての IPsec 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。

**tunnel-group name ipsec-attributes**  
**no tunnel-group name ipsec-attributes**

### 構文の説明

**ipsec-attributes** このトンネルグループの属性を指定します。

**name** トンネルグループの名前を指定します。

### 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
グローバルコンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

### コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

7.1(1) さまざまな IPsec トンネルグループ属性が一般トンネルグループ属性リストに移行され、トンネルグループ ipsec 属性モードのプロンプトが変更されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

### 例

次に、グローバル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 remotegrp のトンネルグループを作成し、その後、IPsec グループ属性を指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)
```

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。

# tunnel-group-list enable

tunnel-group group-alias で定義されているトンネルグループをイネーブルにするには、**tunnel-group-list enable** コマンドを使用します。

## tunnel-group-list 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。

### 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	• 対応	—

### 使用上のガイドライン

このコマンドは、クライアントレスまたは AnyConnect VPN クライアントセッションで tunnel-group group-alias および group-url コマンドと組み合わせて使用します。このコマンドは、ログインページに tunnel-group ドロップダウンが表示されるように機能をイネーブルにします。group-alias は、エンドユーザーに表示するために ASA 管理者が定義した、従業員、技術部門、コンサルタントなどのテキスト文字列です。

### コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

### 例

```
ciscoasa# configure
terminal
ciscoasa(config)# tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)# group-alias Group1 enable
ciscoasa(config-tunnel-webvpn)# exit
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
```

### 関連コマンド

コマンド	説明
tunnel-group	VPN 接続プロファイルを作成するか、または VPN 接続プロファイルのデータベースにアクセスします。

コマンド	説明
group-alias	接続プロファイル（トンネルグループ）のエイリアスを設定します。
group-url	VPN エンドポイントで指定されている URL または IP アドレスと接続プロファイルを照合します。
<b>show running-config tunnel-group</b>	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

適応型セキュリティアプライアンスがIPSec接続要求をクライアント証明書認証とともに受信すると、設定したポリシーに従って接続プロファイルをその接続に割り当てます。

そのポリシーは、設定したルールの使用、証明書のOUフィールドの使用、IKE ID（ホスト名、IPアドレス、キーIDなど）の使用、クライアントのIPアドレス、あるいは接続プロファイルを割り当てるデフォルトの接続プロファイルになります。SSL接続に対し、適応型セキュリティアプライアンスは、接続プロファイルを割り当てるように設定したルールを使用するだけです。

既存のマップ名を接続プロファイルに関連付けて設定したルールに基づき、**tunnel-group-map** コマンドにより、接続プロファイルが接続に割り当てられます。

接続プロファイルとマップ名の関連を解消するには、このコマンドの **no** 形式を使用します。このコマンドの **no** 形式ではマップ名は削除されません。マップ名と接続プロファイルとの関連が解消されるだけです。

コマンドの構文は次のとおりです。

```
tunnel-group-map [ mapname ] [ rule-index ] [ connection-profile ]
no tunnel-group-map [ mapname ] [ rule-index ]
```



- (注)
- 次のコマンドで証明書マップ名を作成します。 `crypto ca certificate map [mapname] [rule-index]`
  - 「トンネルグループ」は、現在「接続プロファイル」と呼ばれている用語の旧称です。 `tunnel-group-map` コマンドは、接続プロファイルマップを作成するものと考えてください。

### 構文の説明

<i>mapname</i>	必須です。既存の証明書マップの名前を指定します。
<i>rule-index</i>	必須です。マップ名に関連付けられた <b>rule-index</b> を指定します。 <b>rule-index</b> パラメータは、 <b>crypto ca certificate map</b> コマンドを使用して定義されます。有効な値は 1 ~ 65535 です。
<i>connection-profile</i>	証明書マップリストに対して接続プロファイル名を指定します。

### コマンドデフォルト

`tunnel-group-map` が未定義で、ASA がIPsec接続リストをクライアント証明書認証とともに受信した場合、ASA は証明書認証要求をこれらのポリシーの1つと次の順序で照合することで、接続プロファイルを割り当てます。

**Certificate ou field** : サブジェクト識別名 (DN) の組織ユニット (OU) フィールドの値に基づき、接続プロファイルを決定します。

**IKE identity—Determines** : フェーズ 1 IKE ID の内容に基づき、接続プロファイルを決定します。**the connection profile based on the**

**peer-ip** : 確立されたクライアント IP アドレスに基づき、接続プロファイルを決定します。**Determines the connection profile based on**

**Default Connection Profile—If the ASA does not match the previous three policies, it assigns the default connection profile. The default profile is DefaultRAGroup. The default connection profile would otherwise be configured using the tunnel-group-map default-group command.**

## コマンドモード

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 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 変更内容  
ス

7.0(1) このコマンドが追加されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

## 使用上のガイドライン

設定したマップ名は、接続プロファイルと関連付ける前に、存在している必要があります。**crypto ca certificate map** コマンドを使用して、マップ名を作成します。詳細については、**crypto ca certificate map** コマンドのマニュアルを参照してください。

マップ名を接続プロファイルに関連付けたら、前述のデフォルトのポリシーではなく設定したルールを使用するには、**tunnel-group-map** をイネーブルにする必要があります。これを行うには、グローバル コンフィギュレーション モードで **tunnel-group-map enable rules** コマンドを実行する必要があります。

## 例

次の例では、rule index が 10 のマップ名 SalesGroup を SalesConnectionProfile 接続プロファイルに関連付けています。

```
ciscoasa(config)# tunnel-group-map SalesGroup 10 SalesConnectionProfile
ciscoasa(config)#
```

## 関連コマンド

コマンド	説明
crypto ca certificate map [map name]	CA 証明書マップ コンフィギュレーション モードを開始し、そのモードを使用して証明書マップ名を作成できます。

コマンド	説明
tunnel-group-map enable	確立されたルールに基づく証明書ベースのIKEセッションをイネーブルにします。
tunnel-group-map default-group	既存のトンネルグループ名をデフォルトのトンネルグループとして指定します。

## tunnel-group-map default-group

tunnel-group-map default-group コマンドでは、他の設定された方式を使用して名前を判別できない場合に使用するデフォルトのトンネルグループを指定します。

tunnel-group-map を削除するには、このコマンドの **no** 形式を使用します。

**tunnel-group-map** [ *rule-index* ] **default-group** *tunnel-group-name*  
**no tunnel-group-map**

### 構文の説明

**default-group**  
*tunnel-group-name* 他の設定された方式では名前を取得できない場合に使用するデフォルトのトンネルグループを指定します。 *tunnel-group name* はすでに存在している必要があります。

*rule index* オプション。 **crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ~ 65535 です。

### コマンド デフォルト

**tunnel-group-map default-group** のデフォルト値は DefaultRAGroup 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 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  
 ス

7.0(1) このコマンドが追加されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

### 使用上のガイドライン

tunnel-group-map コマンドは、証明書ベースの IKE セッションをトンネルグループにマップするときのポリシーおよびルールを設定します。 **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るには、グローバルコンフィギュレーションモードで **tunnel-group-map** コマンドを使用します。各呼び出しが一意であり、マップインデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。

**crypto ca certificate map** コマンドは、証明書マッピングルールの優先順位リストを維持しません。設定できるマップは 1 つだけです。ただし、65535 個までのルールをそのマップに設定で

きます。詳細については、**crypto ca certificate map** コマンドのマニュアルを参照してください。

証明書からトンネルグループ名を取得する処理は、トンネルグループに関連付けられていない証明書マップのエントリを無視します（どのマップルールもこのコマンドでは識別されません）。

## 例

次の例はグローバルコンフィギュレーションモードで入力され、他の設定済みメソッドで名前を取得できない場合に使用されるデフォルトのトンネルグループを指定します。使用するトンネルグループの名前は **group1** です。

```
ciscoasa(config)# tunnel-group-map default-group group1
ciscoasa(config)#
```

## 関連コマンド

コマンド	説明
<b>crypto ca certificate map</b>	クリプト CA 証明書マップ コンフィギュレーション モードを開始します。
subject-name (クリプト CA 証明書マップ)	ルールエントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
<b>tunnel-group-map enable</b>	証明書ベースの IKE セッションをトンネルグループにマップ ping するためのポリシーとルールを設定します。

## tunnel-group-map enable

**tunnel-group-map enable** コマンドでは、証明書ベースの IKE セッションをトンネルグループにマッピングするためのポリシーとルールを設定します。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。

**tunnel-group-map** [ *rule-index* ] **enable** *policy*

**no tunnel-group-map enable** [ *rule-index* ]

### 構文の説明

**ポリシー** 証明書からトンネルグループ名を取得するためのポリシーを指定します。*policy* は次のいずれかです。

**ike-id** : トンネルグループがルールルックアップに基づいて判別されない、または **ou** から取得されない場合は、フェーズ 1 IKE ID の内容に基づいて、証明書ベースの IKE セッションがトンネルグループにマッピングされることを示します。

**ou** : トンネルグループがルールルックアップに基づいて判別されない場合は、サブジェクト認定者名 (DN) の組織ユニット (OU) の値が使用されることを示します。

**peer-ip** : トンネルグループがルールルックアップに基づいて判別されないか、**ou** または **ike-id** メソッドから取得されない場合、確立されたピア IP アドレスが使用されることを示します。

**rules** : このコマンドによって設定された証明書マップの関連付けに基づいて、証明書ベースの IKE セッションがトンネルグループにマッピングされることを示します。

**rule index** (オプション) **crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ~ 65535 です。

### コマンド デフォルト

**tunnel-group-map** コマンドのデフォルト値は **enable ou** で、**default-group** は DefaultRAGroup 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。

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	トランスパレント	シングル	マルチ	
				コンテキスト	システム
グローバル 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  
ス

7.0(1) このコマンドが追加されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

## 使用上のガイドライン

**crypto ca certificate map** コマンドは、証明書マッピングルールの優先順位リストを維持します。設定できるマップは1つだけです。ただし、65535個までのルールをそのマップに設定できます。詳細については、**crypto ca certificate map** コマンドのマニュアルを参照してください。

## 例

次に、フェーズ1 IKE ID の内容に基づく、証明書ベースの IKE セッションとトンネルグループとのマッピングをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group-map enable ike-id
ciscoasa(config)#
```

次に、確立済みのピアの IP アドレスに基づく、証明書ベースの IKE セッションとトンネルグループとのマッピングをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group-map enable peer-ip
ciscoasa(config)#
```

次に、サブジェクト認定者名 (DN) の組織ユニット (OU) に基づく、証明書ベースの IKE セッションのマッピングをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group-map enable ou
ciscoasa(config)#
```

次に、確立済みのルールに基づく証明書ベースの IKE セッションのマッピングをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group-map enable rules
ciscoasa(config)#
```

## 関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
subject-name (クリプト CA 証明書マップ)	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map default-group	既存のトンネルグループ名をデフォルトのトンネルグループとして指定します。

## tunnel-group ppp-attributes

ppp 属性コンフィギュレーションモードを開始し、IPsec を介した L2TP 接続によって使用される PPP 設定値を設定するには、グローバル コンフィギュレーション モードで **tunnel-group ppp-attributes** コマンドを使用します。

すべての PPP 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。

**tunnel-group name ppp-attributes**  
**no tunnel-group name ppp-attributes**

### 構文の説明

*name* トンネルグループの名前を指定します。

### 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
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

### コマンド履歴

リリース 変更内容  
 ス

7.2(1) このコマンドが追加されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

### 使用上のガイドライン

PPP 設定値はレイヤ 2 トンネリングプロトコル (L2TP) によって使用されます。L2TP は、リモートクライアントがダイヤルアップ電話サービスのパブリック IP ネットワークを使用してプライベート社内ネットワーク サーバーとセキュアに通信できるようにする VPN トンネリングプロトコルです。L2TP はクライアント/サーバー モデルに基づき、PPP over UDP (ポート 1701) を使用してデータをトンネルします。tunnel-group ppp コマンドはすべて、PPPoE トンネルグループタイプで使用できます。

### 例

次に、トンネルグループ *telecommuters* を作成し、ppp 属性コンフィギュレーションモードを開始する例を示します。

```
ciscoasa(config)# tunnel-group telecommuters type pppoe
```



```
ciscoasa(config)# tunnel-group telecommuters ppp-attributes
ciscoasa(tunnel-group-ppp)#
```

## 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。

# tunnel-group-preference

エンドポイントで指定された URL と一致するグループ URL を含む接続プロファイルに VPN プリファレンスを変更するには、`webvpn` コンフィギュレーションモードで **tunnel-group-preference** 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するには、`no` 形式を使用します。

**tunnel-group-preference group-url**  
**no tunnel-group-preference group-url**

## 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、接続プロファイルで指定された証明書のフィールド値とエンドポイントで使用する証明書のフィールド値が ASA によって照合され、一致した場合は、そのプロファイルが VPN 接続に割り当てられます。このコマンドは、デフォルトの動作を上書きします。

## 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
config-webvpn	• 対応	—	• 対応	—	—

## コマンド履歴

リリース 変更内容

8.2(5)/8.4(2) このコマンドが追加されました。

## 使用上のガイドライン

このコマンドは、接続プロファイルの選択プロセス中に、接続プロファイルのプリファレンスを変更します。これにより、ASA ソフトウェアの数多くの旧リリースによって使用されるグループ URL プリファレンスを利用できます。エンドポイントによって、接続プロファイルにないグループ URL が指定され、かつ接続プロファイルの証明書値と一致する証明書値が指定されている場合、ASA ではその接続プロファイルを VPN セッションに割り当てます。

このコマンドは `webvpn` コンフィギュレーションモードで入力しますが、このコマンドによって、ASA によってネゴシエートされたすべてのクライアントレスおよび AnyConnect VPN 接続について、接続プロファイルの選択プリファレンスが変更されます。

## 例

次に、接続プロファイルの選択プロセス中に、接続プロファイルのプリファレンスを変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-preference group-url
ciscoasa(config-webvpn)#
```

## 関連コマンド

コマンド	説明
tunnel-group	VPN 接続プロファイルを作成するか、または VPN 接続プロファイルのデータベースにアクセスします。
group-url	VPN エンドポイントで指定されている URL または IP アドレスと接続プロファイルを照合します。
<b>show running-config</b> <b>tunnel-group</b>	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 webvpn-attributes

WebVPN 属性コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **tunnel-group webvpn-attributes** コマンドを使用します。このモードでは、WebVPN トンネリングに共通の設定値を設定します。

すべての WebVPN 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。

**tunnel-group name webvpn-attributes**  
**no tunnel-group name webvpn-attributes**

### 構文の説明

**name** トンネルグループの名前を指定します。

(注) トンネルグループ名に次の特殊文字が含まれていないことを確認してください。&、"、または<

**webvpn-attributes** このトンネルグループの WebVPN 属性を指定します。

### 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
グローバルコンフィギュレーション	• 対応	—	• 対応	• 対応	—

### コマンド履歴

リリース 変更内容

7.1(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。

9.8(1) `pre-fill-username` および `secondary-pre-fill-username` の値が `clientless` から `client` に変更されました。

### 使用上のガイドライン

一般属性に加えて、webvpn 属性モードで WebVPN 接続に固有の次の属性も設定できます。

- authentication
- customization

- dns-group
- group-alias
- group-url
- without-csd

pre-fill-username および secondary-pre-fill-username 属性は、認証および認可に使用する証明書からユーザー名を抽出するために使用されます。値は client または clientless です。

## 例

次に、グローバル コンフィギュレーション モードを開始し、LAN-to-LAN ピアの IP アドレスを使用して WebVPN 接続用のトンネルグループを作成し、その後、WebVPN 属性を設定するための webvpn コンフィギュレーション モードを開始する例を示します。トンネルグループの名前は、209.165.200.225 です。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type webvpn
ciscoasa(config)# tunnel-group 209.165.200.225 webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

次に、グローバル コンフィギュレーション モードで、WebVPN 接続用のトンネルグループ「remotegrp」を作成し、その後、トンネルグループ「remotegrp」の WebVPN 属性を設定するための webvpn コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type webvpn
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

## 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。

# tunnel-limit

許可されるアクティブな GTP トンネルの最大数を指定するには、ポリシーマップパラメータコンフィギュレーションモードで **tunnel limit** コマンドを使用します。トンネル制限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。

**tunnel-limit** *max\_tunnels*  
**no tunnel-limit** *max\_tunnels*

## 構文の説明

*max\_tunnels* 許可されるトンネルの最大数。これは、PDP コンテキストまたはエンドポイントの数の相当します。

## コマンド デフォルト

デフォルトのトンネル制限値は 500 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
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 変更内容  
 ス

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

このコマンドで指定したトンネル数に達すると、新しい要求はドロップされます。

## 例

次に、GTP トラフィックの最大トンネル数を 10,000 に指定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
```

```
ciscoasa(config-pmap)# parameters
```

```
ciscoasa(config-pmap-p)# tunnel-limit 10000
```

## 関連コマンド

コマンド	説明
<b>clear service-policy inspect gtp</b>	グローバルな GTP 統計情報をクリアします。

コマンド	説明
<b>inspect gtp</b>	アプリケーションインスペクションに使用する特定のGTPマップを適用します。
<b>show service-policy inspect gtp</b>	GTP コンフィギュレーションを表示します。

## tx-ring-limit

プライオリティキューの深さを指定するには、プライオリティキューモードで **tx-ring-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。



- (注) このコマンドは ASA 5580 10 ギガビットイーサネットインターフェイス、ASA 5512-X ~ ASA 5555-X 管理インターフェイス、または ASA サービス モジュールではサポートされません (10 ギガビットイーサネットインターフェイスは、ASA 5585-X のプライオリティキューに対してサポートされます)。

**tx-ring-limit** *number-of-packets*  
**no tx-ring-limit** *number-of-packets*

### 構文の説明

*number-of-packets* イーサネット送信ドライバが許容できる低遅延パケットまたは標準のプライオリティのパケットの最大数を指定します。このパケットの処理が終わると、イーサネット送信ドライバは輻輳が解消するまで、インターフェイス上のパケットをバッファしているキューの処理に戻ります。指定できる範囲は 3 ~ 511 です。

### コマンドデフォルト

デフォルト値は 511 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
プライオリティキュー	• 対応	• 対応	• 対応	• 対応	—

### コマンド履歴

リリー 変更内容  
 ス

7.0(1) このコマンドが追加されました。

### 使用上のガイドライン

ASA では、遅延の影響を受けやすい、プライオリティの高いトラフィック (音声およびビデオなど) 用の低遅延キューイング (LLQ) と、それ以外のトラフィック用のベストエフォート (デフォルト) という 2 つのトラフィッククラスを使用できます。ASA は、プライオリティトラフィックを認識して、適切な Quality of Service (QoS) ポリシーを適用します。プライオリティキューのサイズと深さを設定して、トラフィックフローを微調整できます。



プライオリティキューイングを有効にする前に、**priority-queue** コマンドを使用して、インターフェイスのプライオリティキューを作成する必要があります。1つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

**priority-queue** コマンドで、プライオリティキューモードを開始します。これはプロンプトに表示されます。プライオリティキューモードでは、いつでも送信キューに入れることができるパケットの最大数 (**tx-ring-limit** コマンド)、およびパケットをドロップする前にバッファに入れることができるいずれかのタイプ (プライオリティまたはベストエフォート) のパケット数 (**queue-limit** コマンド) を設定できます。

指定する **tx-ring-limit** および **queue-limit** は、プライオリティの高い低遅延キューとベストエフォートキューの両方に適用されます。**tx-ring-limit** は、ドライバが許容できる両方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。通常、これらの2つのパラメータを調整することで、低遅延トラフィックのフローを最適化できます。

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。これがテールドロップです。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファサイズを大きくします。



(注) **queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この制限を表示するには、コマンドラインで **help** または **?** を入力します。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。

ASA モデル 5505 (のみ) では、1つのインターフェイスに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で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。さらに、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も削除されます。

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。

## 例

次の例では、**test** というインターフェイスにプライオリティキューを、キュー制限を2048パケットに、送信キュー制限を256パケットに設定しています。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 2048
ciscoasa(priority-queue)# tx-ring-limit 256
```

関連コマンド	コマンド	説明
	<b>clear configure priority-queue</b>	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
	<b>priority-queue</b>	インターフェイスにプライオリティキューイングを設定します。
	<b>queue-limit</b>	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。
	<b>show priority-queue statistics</b>	指定されたインターフェイスのプライオリティ キュー統計情報を表示します。
	<b>show running-config priority-queue</b>	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。 <b>all</b> キーワードを指定した場合、このコマンドは、現在の <b>priority-queue</b> 、 <b>queue-limit</b> 、および <b>tx-ring-limit</b> コマンドのコンフィギュレーション値をすべて表示します。

# type echo

SLA 動作をエコー応答時間プローブ動作として設定するには、SLA モニターコンフィギュレーションモードで **type echo** コマンドを使用します。SLA コンフィギュレーションから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。

**type echo protocol ipIcmpEcho target interface if-name**  
**no type echoprotocol ipIcmpEcho target interface if-name**

## 構文の説明

<b>interface</b> <i>if-name</i>	エコー要求パケットを送信するために使用されるインターフェイスのインターフェイス名を、 <b>nameif</b> コマンドで指定されているとおりに指定します。インターフェイス送信元アドレスが、エコー要求パケットの送信元アドレスとして使用されます。
<b>protocol</b>	プロトコルのキーワード。サポートされる唯一の値が <b>ipIcmpEcho</b> で、エコー動作で IP/ICMP エコー要求を使用するように指定します。
<b>target</b>	モニターするオブジェクトの IP アドレスまたはホスト名。

## 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
SLA モニター コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

## コマンド履歴

リリー 変更内容  
ス

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

ICMP パケットのペイロードのデフォルト サイズは 28 バイトで、合計サイズが 64 バイトの ICMP パケットを作成します。ペイロードサイズは、**request-data-size** コマンドを使用して変更できます。

## 例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。SLA の到達可能性を追跡するために、ID が 1 のトラッキング

エントリを作成します。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

#### 関連コマンド

コマンド	説明
<b>num-packets</b>	SLA 動作中に送信する要求パケットの数を指定します。
<b>request-data-size</b>	SLA 動作要求パケットのペイロードのサイズを指定します。
<b>sla monitor</b>	SLA モニタリング動作を定義します。

## 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。