tls-proxy コマンド～ type echo コマンド

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

max_sessions *max_sessions*	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。
noconfirm	確認を要求せずに **tls-proxy** コマンドを実行します。
proxy_name	TLS プロキシ インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

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
クライアント	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキー ペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
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。

token

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。

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。

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

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
public-key	Cisco Umbrella で使用する公開キーを設定します。
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からの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。
umbrella-global	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 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
SLA モニタ 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
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
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
request-data-size	要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。
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

destination_ip	traceroute 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。
hostname	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、**name** コマンドで定義するか、traceroute 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。
max-ttl	使用可能な最大 TTL 値。デフォルトは 30 です。traceroute 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。
min_ttl	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。
numeric	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。
port *port_value*	ユーザ 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。
probe *probe_num*	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。
source	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。
source_interface	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。
source_ip	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。
timeout	使用されるタイムアウト値を指定します。
timeout_value	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。
ttl	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。
use-icmp	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。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
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

traceroute コマンドは送信した各プローブの結果を示します。出力の各行が 1 つの TTL 値に対応します(昇順)。次に、**traceroute** 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	各ノードに対する、指定した数のプローブのラウンドトリップ時間(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 が設定によって禁止されています。
?	ICMP の原因不明の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 traceroute 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
capture	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。
show capture	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。
packet-tracer	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。

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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 は、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トを表示します。

表 2-1　SLA 追跡の戻りコード

トラッキング	戻りコード	追跡ステート
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
route	スタティック ルートを設定します。
sla monitor	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専用モードに設定します。モニタ専用モードでは、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。

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

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。
9.2(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用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 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。
- 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、GigabitEthernet 0/5 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
interface	インターフェイス コンフィギュレーション モードを開始します。
cxsc	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。
sfr	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。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップで既知の 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
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。

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。

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

アクション	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。
allow	メッセージを許可します。
chunked	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。
compress	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。
デフォルト	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。
deflate	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。
drop	接続を閉じます。
gzip	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。
identity	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。
ログ	（任意）syslog を生成します。
reset	TCP リセット メッセージをクライアントおよびサーバに送信します。
type	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。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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**デフォルト**のアクションを適用します。設定済みの**デフォルト**のアクションでは、ロギングなしで接続を**許可**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 タイプそれぞれに **allow** アクションを設定します。

適用する各設定に対して 1 回ずつ **transfer-encoding** コマンドを入力します。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
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

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）（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 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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。ASA は現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

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 サーバの運用統計情報を表示します。
sso server	SSO サーバのタイプを作成、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 サーバの認証を可能にする信頼検証サービス サーバを指定するには、SIP インスペク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。

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 サーバの IP アドレスを指定します。SIP インスペクション 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 インスペクションは、登録された電話機ごとに各サーバへのピンホールを開き、電話機はどのサーバを使用するかを決定します。Cisco Unified Communications Manager（CUCM）サーバで、信頼検証サービス サーバを設定します。
port *number*	サーバ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。

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。

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

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、SIP インスペクション 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
policy-map type inspect	インスペクション ポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

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。
ログ	システム メッセージ ログを生成します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

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 の存在のモニタと強制をイネーブルにします。

例

次に、DNS インスペクション 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
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。

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。

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。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **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 ホストにとっては、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
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

tunnel destination

VTI トンネルの宛先の IP アドレスを指定するには、インターフェイス コンフィギュレーション モードで **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 address	VTI トンネルの宛先の IP アドレス（IPv4）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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

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
interface tunnel	新しい VTI トンネル インターフェイスを作成します。
tunnel source interface	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。
トンネル モード	IPsec がトンネル保護に使用されることを指定します。
tunnel protection ipsec	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。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*

no tunnel mode *ipsec IPv4*

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

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
interface tunnel	新しい VTI トンネル インターフェイスを作成します。
tunnel source interface	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。
tunnel destination	VTI トンネルの宛先の IP アドレスを指定します。
tunnel protection ipsec	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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

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
interface tunnel	新しい VTI トンネル インターフェイスを作成します。
tunnel source interface	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。
tunnel destination	VTI トンネルの宛先の IP アドレスを指定します。
トンネル モード	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*

no tunnel source interface *interface name*

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

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
interface tunnel	新しい VTI トンネル インターフェイスを作成します。
tunnel destination	VTI トンネルの宛先の IP アドレスを指定します。
トンネル モード	IPsec がトンネル保護に使用されることを指定します。
tunnel protection ipsec	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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

使用上のガイドライン

SSL VPN ユーザ（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 接続に対して、ASA は、トンネル グループを、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 グループの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-l2l
```

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-l2l
```

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
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。
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。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。

tunnel-group-map

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）

- このコマンドで証明書マップ名を作成できます。
  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

mapname	必須です。既存の証明書マップの名前を指定します。
rule-index	必須です。マップ名に関連付けられた rule-index を指定します。rule-index パラメータは、**crypto ca certificate map** コマンドを使用して定義されます。有効な値は 1 ～ 65535 です。
connection-profile	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。

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。

証明書の ou フィールド：サブジェクト Distinguish Name（DN; 認定者名）の Organizational Unit（OU; 組織ユニット）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 ID：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。

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。

デフォルト接続プロファイル：ASA が上記 3 つのポリシーに一致しない場合は、デフォルトの接続プロファイルを割り当てます。デフォルトのプロファイルは DefaultRAGroup です。そうでない場合は、デフォルトの接続プロファイルは、tunnel-group-map default-group コマンドを使用して設定されます。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
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** コマンドの資料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。
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。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	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保守します。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** コマンドの資料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
crypto ca certificate map	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。
tunnel-group-map enable	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。

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 セッションをトンネル 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 グループが規則の検索に基づいて決定されないか、ou または ike-id 方式から取得されない場合、確立されたピア IP アドレスを使用することを示します。 **rules**：このコマンドによって設定された証明書マップ アソシエーションに基づいて、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	（任意）**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。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	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保守します。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** コマンドの資料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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
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 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され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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
config-webvpn	• 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。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(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に相当します。

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。

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

コマンド履歴

リリース	変更内容
7.0(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
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
inspect gtp	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。
show service-policy inspect gtp	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。

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。

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

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA では、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、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）の 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、実行時にダイナミックに決定されます。この制限を表示するには、コマンドラインに **help** または **?** と入力します。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
clear configure priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
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
show priority-queue statistics	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。
show running-config 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** キーワードを指定した場合、このコマンドは、現在の **priority-queue**、**queue-limit**、および **tx-ring-limit** 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 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

interface *if-name*	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、**nameif** 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。
protocol	プロトコルのキーワード。サポートされる唯一の値が **ipIcmpEcho** 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。
target	モニタするオブジェクトの IP アドレスまたはホスト名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
request-data-size	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。
sla monitor	SLA モニタリング動作を定義します。