CHAPTER 31

shun コマンド～ sysopt radius ignore-secret コマンド

shun

攻撃元ホストからの接続をブロックするには、特権 EXEC モードで **shun** コマンドを使用します。shun をディセーブルにするには、このコマンドの **no** 形式を使用します。

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

構文の説明

dest_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先ポートを指定します。
dest_ip	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先アドレスを指定します。
protocol	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の IP プロトコル（UDP や TCP など）を指定します。デフォルトでは、プロトコルは 0（すべてのプロトコル）です。
source_ip	攻撃元ホストのアドレスを指定します。送信元 IP アドレスのみを指定した場合、このアドレスからの今後のすべての接続はドロップされます。現在の接続はそのまま維持されます。現在の接続をドロップし、かつ shun を適用するには、その接続についての追加パラメータを指定します。その送信元 IP アドレスからの今後のすべての接続には、宛先パラメータに関係なく、shun がそのまま維持されます。
source_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする、現在の接続の送信元ポートを指定します。
vlan_id	（任意）送信元ホストが配置されている VLAN ID を指定します。

デフォルト

デフォルトのプロトコルは 0（すべてのプロトコル）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

shun コマンドを使用すると、攻撃元ホストからの接続をブロックできます。送信元 IP アドレスからの今後のすべての接続は、手動または Cisco IPS センサーによってブロッキング機能が削除されるまで、ドロップされ、ログに記録されます。**shun** コマンドのブロッキング機能は、指定したホスト アドレスとの接続が現在アクティブかどうかに関係なく適用されます。

宛先アドレス、送信元ポート、宛先ポート、およびプロトコルを指定すると、一致する接続がドロップされ、かつ、その送信元 IP アドレスからの今後のすべての接続に shun が適用されます。この場合、これらの特定の接続パラメータと一致する接続だけでなく、今後のすべての接続が回避されます。

shun コマンドは、送信元 IP アドレスごとに 1 つのみ使用できます。

shun コマンドは攻撃をダイナミックにブロックするために使用されるため、セキュリティ アプライアンス コンフィギュレーションには表示されません。

インターフェイス コンフィギュレーションが削除されると、そのインターフェイスに付加されているすべての shun も削除されます。新しいインターフェイスを追加するか、または同じインターフェイスを（同じ名前を使用して）置き換える場合、IPS センサーでそのインターフェイスをモニタするには、そのインターフェイスを IPS センサーに追加する必要があります。

例

次に、攻撃ホスト（10.1.1.27）が攻撃対象（10.2.2.89）に TCP で接続する例を示します。この接続は、セキュリティ アプライアンス接続テーブル内で次のように記載されています。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

次のオプションを使用して、**shun** コマンドを適用します。

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

このコマンドにより、現在の接続はセキュリティ アプライアンス接続テーブルから削除され、10.1.1.27 からの今後のすべてのパケットはセキュリティ アプライアンスを通過できなくなります。

関連コマンド

コマンド	説明
clear shun	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
show conn	すべてのアクティブな接続を表示します。
show shun	回避についての情報を表示します。

shutdown

インターフェイスをディセーブルにするには、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを使用します。インターフェイスをイネーブルにするには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

すべての物理インターフェイスは、デフォルトではシャットダウンされます。セキュリティ コンテキスト内の割り当て済みのインターフェイスは、コンフィギュレーション内でシャットダウンされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

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

使用上のガイドライン

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

（注）　このコマンドでは、ソフトウェア インターフェイスのみがディセーブルになります。物理リンクはアップのまま維持され、対応するインターフェイスが **shutdown** コマンドを使用して設定された場合でも、直接接続されたデバイスはアップであると認識されます。

例

次に、メイン インターフェイスをイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

次に、サブインターフェイスをイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次に、サブインターフェイスをシャットダウンする例を示します。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に対するすべての変換をリセットして、その結果として接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

shutdown（ca-server モード）

ローカル Certificate Authority（CA; 認証局）サーバをディセーブルにし、ユーザが登録インターフェイスにアクセスできないようにするには、CA サーバ コンフィギュレーション モードで **shutdown** コマンドを使用します。CA サーバをイネーブルにし、コンフィギュレーションをロックして変更できないようにし、登録インターフェイスにアクセスできるようにするには、このコマンドの **no** 形式を使用します。

[no] shutdown

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

最初は、CA サーバはデフォルトでシャットダウンされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CA サーバ モードのこのコマンドは、インターフェイス モードの **shutdown** コマンドと類似しています。セットアップ時に、ローカル CA サーバはデフォルトでシャットダウンされるため、**no shutdown** コマンドを使用してイネーブルにする必要があります。**no shutdown** コマンドを初めて使用するときは、CA サーバをイネーブルにし、CA サーバ証明書とキー ペアを生成します。

（注）　**no shutdown** コマンドを発行することによって、CA コンフィギュレーションをロックして CA 証明書を生成した後は、CA コンフィギュレーションを変更できません。

no shutdown コマンドで CA サーバをイネーブルにして現在のコンフィギュレーションをロックするには、生成される CA 証明書とキー ペアが含まれる PKCS12 ファイルを符号化してアーカイブするために、7 文字のパスワードが必要です。このファイルは、以前に指定した **database path** コマンドで識別されるストレージに格納されます。

例

次に、ローカル CA サーバをディセーブルにし、登録インターフェイスにアクセスできないようにする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# shutdown
```

```
hostname(config-ca-server)#
```

次に、ローカル CA サーバをイネーブルにし、登録インターフェイスにアクセスできるようにする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no shutdown
hostname(config-ca-server)#

hostname(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin. Please wait...

hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
show crypto ca server	CA コンフィギュレーションのステータスを表示します。

sla monitor

SLA 動作を作成するには、グローバル コンフィギュレーション モードで **sla monitor** コマンドを使用します。SLA 動作を削除するには、このコマンドの **no** 形式を使用します。

sla monitor *sla_id*

no sla monitor *sla_id*

構文の説明

sla_id	設定する SLA の ID を指定します。SLA が存在しない場合は、作成されます。有効な値は 1 ～ 2147483647 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

sla monitor コマンドによって、SLA 動作が作成され、SLA モニタ コンフィギュレーション モードが開始されます。このコマンドを入力すると、コマンド プロンプトは `hostname(config-sla-monitor)#` に変わり、SLA モニタ コンフィギュレーション モードになったことが示されます。SLA 動作がすでに存在し、それに対してタイプがすでに定義されている場合、プロンプトは `hostname(config-sla-monitor-echo)#` と表示されます。最大 2000 個の SLA 動作を作成できます。任意の時点でデバッグできるのは 32 個の SLA 動作のみです。

no sla monitor コマンドによって、指定した SLA 動作およびその動作を設定するために使用されたコマンドが削除されます。

SLA 動作を設定した後、**sla monitor schedule** コマンドで動作をスケジューリングする必要があります。スケジューリング後は、SLA 動作のコンフィギュレーションを変更できません。スケジューリングした SLA 動作のコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択した SLA 動作を完全に削除する必要があります。SLA 動作を削除すると、関連づけられた **sla monitor schedule** コマンドも削除されます。その後、SLA 動作のコンフィギュレーションを再入力できます。

動作の現在のコンフィギュレーション設定を表示するには、**show sla monitor configuration** コマンドを使用します。SLA 動作の動作統計情報を表示するには、**show sla monitor operation-state** コマンドを使用します。コンフィギュレーション内の SLA コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

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

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA 動作を繰り返す頻度を指定します。
show sla monitor configuration	SLA コンフィギュレーション設定を表示します。
sla monitor schedule	SLA 動作をスケジューリングします。
timeout	SLA 動作が応答を待機する時間を設定します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

sla monitor schedule

SLA 動作をスケジューリングするには、グローバル コンフィギュレーション モードで **sla monitor schedule** コマンドを使用します。SLA 動作のスケジュールを削除し、動作を保留状態にするには、このコマンドの **no** 形式を使用します。

sla monitor schedule *sla-id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no sla monitor schedule *sla-id*

構文の説明

after *hh*:*mm*:*ss*	コマンドの入力後、何時間、何分、何秒で動作が開始されるかを示します。
ageout *seconds*	（任意）情報をアクティブに収集していない場合、動作をメモリに常駐させておく時間を秒数で指定します。エージング アウト後、SLA 動作は実行コンフィギュレーションから削除されます。
day	動作を開始する日。有効な値は、1 ～ 31 です。日を指定しない場合、現在の日が使用されます。日を指定する場合は、月も指定する必要があります。
hh:*mm*[:*ss*]	絶対開始時刻を 24 時間表記で指定します。秒は任意です。*month* および *day* を指定しない場合は、指定した時刻が次に来たときとなります。
life forever	（任意）無期限に実行されるように動作をスケジューリングします。
life *seconds*	（任意）動作によって情報がアクティブに収集される秒数を設定します。
month	（任意）動作を開始する月の名前。月を指定しない場合、現在の月が使用されます。月を指定する場合は、日も指定する必要があります。 月の英語名を完全に入力するか、または、最初の 3 文字のみを入力します。
now	コマンドを入力するとすぐに動作が開始されることを示します。
pending	情報が収集されないことを示します。これは、デフォルトの状態です。
recurring	（任意）動作が毎日、指定した時刻に自動的に開始され、指定した時間継続されることを示します。
sla-id	スケジューリングする SLA 動作の ID。
start-time	SLA 動作が開始される時刻を設定します。

デフォルト

デフォルトの設定は次のとおりです。

- SLA 動作は、スケジューリングされた時間になるまで **pending** 状態です。つまり、動作はイネーブルですが、データはアクティブに収集されていません。
- デフォルトの **ageout** 時間は、0 秒（エージング アウトしない）です。
- デフォルトの **life** は、3600 秒（1 時間）です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　SLA 動作がアクティブ状態の場合、ただちに情報の収集が開始されます。次のタイム ラインは、動作のエージング アウト プロセスを示しています。

```
W----------------------X----------------------Y----------------------Z
```

- W は、SLA 動作が **sla monitor** コマンドで設定された時刻です。
- X は、SLA 動作の開始時刻です。これは、動作が「アクティブ」になったときです。
- Y は、**sla monitor schedule** コマンドで設定された有効期間の終了です（**life** の秒数は 0 までカウント減少されました）。
- Z は、動作のエージング アウトです。

エージング アウト プロセスが使用される場合、エージング アウト プロセスは、W でカウントダウンを開始し、X と Y の間は中断され、Y で設定されたサイズにリセットされてカウントダウンを再開します。SLA 動作がエージング アウトすると、SLA 動作のコンフィギュレーションは実行コンフィギュレーションから削除されます。動作は、実行される前にエージング アウトする可能性があります（つまり、Z が X の前に発生する可能性があります）。このような状況が発生しないようにするには、動作のコンフィギュレーション時刻と開始時刻（X と W）の差を、エージング アウトの秒数よりも小さくする必要があります。

recurring キーワードは、単一の SLA 動作のスケジューリングに対してのみサポートされています。1 つの **sla monitor schedule** コマンドを使用して複数の SLA 動作をスケジューリングすることはできません。定期的な SLA 動作の **life** 値は、1 日未満にする必要があります。定期的な動作の **ageout** 値を「なし」（値 0 で指定）にするか、**life** 値と **ageout** 値の合計を 1 日よりも大きくする必要があります。recurring オプションを指定しないと、動作は既存の通常のスケジューリング モードで開始されます。

スケジューリング後は、SLA 動作のコンフィギュレーションを変更できません。スケジューリングした SLA 動作のコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択した SLA 動作を完全に削除する必要があります。SLA 動作を削除すると、関連づけられた **sla monitor schedule** コマンドも削除されます。その後、SLA 動作のコンフィギュレーションを再入力できます。

例　次に、4 月 5 日午後 3 時にデータの収集をアクティブに開始するようにスケジューリングされた SLA 動作 25 の例を 示します。この動作は、非アクティブになって 12 時間後にエージング アウトします。この SLA 動作がエージング アウトすると、SLA 動作のすべてのコンフィギュレーション情報は実行コンフィギュレーションから削除されます。

```
hostname(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

次に、5 分間の遅延の後にデータの収集を開始するようにスケジューリングされた SLA 動作 1 の例を示します。デフォルトの有効期間である 1 時間が適用されます。

```
hostname(config)# sla monitor schedule 1 start after 00:05:00
```

次に、ただちにデータの収集を開始するようにスケジューリングされた SLA 動作 3 の例を示します。この例は、無期限に実行されるようにスケジューリングされています。

```
hostname(config)# sla monitor schedule 3 life forever start-time now
```

次に、毎日午前 1 時 30 分にデータの収集を自動的に開始するようにスケジューリングされた SLA 動作 15 の例を示します。

```
hostname(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

関連コマンド

コマンド	説明
show sla monitor configuration	SLA コンフィギュレーション設定を表示します。
sla monitor	SLA モニタリング動作を定義します。

smart-tunnel auto-signon enable

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル自動サインオンをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel auto-signon enable** コマンドを使用します。

[**no**] **smart-tunnel auto-signon enable** *list* [**domain** *domain*]

グループ ポリシーまたはユーザ名から **smart-tunnel auto-signon enable** コマンドを削除し、デフォルトのグループ ポリシーから継承するには、このコマンドの **no** 形式を使用します。

構文の説明

list	*list* は、セキュリティ アプライアンスの webvpn コンフィギュレーションにすでに存在するスマート トンネル自動サインオン リストの名前です。 SSL VPN コンフィギュレーション内のスマート トンネル自動サインオン リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。
domain *domain*	（任意）認証中にユーザ名に追加されるドメインの名前。ドメインを入力する場合、**use-domain** キーワードをリスト エントリに入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

スマート トンネル自動サインオン機能は、Microsoft WININET ライブラリを使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。

smart-tunnel auto-signon *list* コマンドを使用して、最初にサーバのリストを作成する必要があります。グループ ポリシーまたはユーザ名に割り当てることができるリストは 1 つだけです。

例

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-signon enable HR
hostname(config-group-webvpn)
```

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをイネーブルにし、認証中に CISCO という名前のドメインをユーザ名に追加します。

```
hostname(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル自動サインオン リスト コマンドを継承します。

```
hostname(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

関連コマンド

コマンド	説明
smart-tunnel auto-signon *list*	スマート トンネル接続でクレデンシャルの送信を自動化する対象のサーバのリストを作成します。
show running-config webvpn smart-tunnel	セキュリティ アプライアンスのスマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel *list*	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel auto-signon list

スマート トンネル接続でクレデンシャルの送信を自動化する対象のサーバのリストを作成するには、webvpn コンフィギュレーション モードで **smart-tunnel auto-signon list** コマンドを使用します。

[**no**] **smart-tunnel auto-signon** *list* [**use-domain**] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

リストに追加する各サーバに対してこのコマンドを使用します。リストからエントリを削除するには、このコマンドの **no** 形式を使用します。リストと、セキュリティ アプライアンス コンフィギュレーションに表示されている IP アドレスまたはホスト名を指定します。スマート トンネル自動サインオン リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。

サーバのリスト全体をセキュリティ アプライアンス コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用して、リストのみを指定します。

no smart-tunnel auto-signon *list*

構文の説明

host	ホスト名またはワイルドカード マスクによって識別されるサーバ。
hostname-mask	自動認証する対象のホスト名またはワイルドカード マスク。
ip	IP アドレスおよびネット マスクによって識別されるサーバ。
ip-address [*netmask*]	自動認証する対象のホストのサブネットワーク。
list	リモート サーバのリストの名前。スペースを含む場合、名前の前後に引用符を使用します。文字列は最大 64 文字まで使用できます。コンフィギュレーション内にリストが存在しない場合は、セキュリティ アプライアンスによって作成されます。存在する場合、リストにエントリを追加します。
use-domain	（任意）認証で必要な場合、Windows ドメインをユーザ名に追加します。このキーワードを入力する場合は、スマート トンネル リストを 1 つ以上のグループ ポリシーまたはユーザ名に割り当てるときにドメイン名を指定してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

スマート トンネル自動サインオン機能は、Microsoft WININET ライブラリを使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。

スマート トンネル自動サインオン リストの入力に続き、グループ ポリシー webvpn モードまたはユーザ名 webvpn モードで **smart-tunnel auto-signon enable** *list* コマンドを使用してリストを割り当てます。

例

次のコマンドでは、サブネット内のすべてのホストを追加し、認証で必要な場合に Windows ドメインをユーザ名に追加します。

```
asa2(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56 255.255.255.0
```

次のコマンドは、リストからエントリを削除します。

```
asa2(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

前述のコマンドでは、削除されるエントリがリストの唯一のエントリである場合、HR という名前のリストも削除されます。唯一のエントリではない場合は、次のコマンドによってリスト全体がセキュリティ アプライアンス コンフィギュレーションから削除されます。

```
asa2(config-webvpn)# no smart-tunnel auto-signon HR
```

次のコマンドでは、ドメイン内のすべてのホストを intranet という名前のスマート トンネル自動サインオン リストに追加します。

```
asa2(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

次のコマンドは、リストからエントリを削除します。

```
asa2(config-webvpn)# no smart-tunnel auto-signon intranet host *.exampledomain.com
```

関連コマンド

コマンド	説明
smart-tunnel auto-signon enable	コマンド モードで指定されたグループ ポリシーまたはユーザ名に対して、スマート トンネル自動サインオンをイネーブルにします。
smart-tunnel auto-signon enable *list*	グループ ポリシーまたはユーザ名にスマート トンネル自動サインオン リストを割り当てます。
show running-config webvpn smart-tunnel	スマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。

smart-tunnel auto-start

クライアントレス（ブラウザベース）SSL VPN セッションでユーザがログインしたときにスマート トンネル アクセスを自動的に開始するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel auto-start** コマンドを使用します。

smart-tunnel auto-start *list*

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除し、デフォルト グループ ポリシーの [**no**] **smart-tunnel** コマンドを継承するには、コマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

list	*list* は、セキュリティ アプライアンス webvpn コンフィギュレーションにすでに存在するスマート トンネル リストの名前です。 SSL VPN コンフィギュレーション内にすでに存在するスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、**smart-tunnel list** コマンドを使用して、最初にアプリケーションのリストを作成する必要があります。

例

次のコマンドでは、apps1 という名前のアプリケーションのリストについて、スマート トンネル アクセスを開始します。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-start apps1
hostname(config-group-webvpn)
```

次のコマンドでは、apps1 という名前のリストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル コマンドを継承します。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no smart-tunnel
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN コンフィギュレーションを、すべてのスマート トンネル リスト エントリを含めて表示します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel disable

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル アクセスを禁止するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel disable** コマンドを使用します。

smart-tunnel disable

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除して、デフォルトのグループ ポリシーから [**no**] **smart-tunnel** コマンドを継承するには、このコマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトではスマート トンネルはイネーブルではないため、**smart-tunnel disable** コマンドは（デフォルトの）グループ ポリシーまたはユーザ名コンフィギュレーションに、対象のポリシーまたはユーザ名に適用しない **smart-tunnel auto-start** または **smart-tunnel enable** コマンドが含まれている場合にのみ必要です。

例

次のコマンドでは、スマート トンネル アクセスを禁止します。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel disable
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel enable

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル アクセスをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel enable** コマンドを使用します。

smart-tunnel enable *list*

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除し、デフォルト グループ ポリシーの [**no**] **smart-tunnel** コマンドを継承するには、コマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

list	*list* は、セキュリティ アプライアンス webvpn コンフィギュレーションにすでに存在するスマート トンネル リストの名前です。 SSL VPN コンフィギュレーション内のスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

smart-tunnel enable コマンドによって、スマート トンネル アクセスに適格なアプリケーションのリストがグループ ポリシーまたはユーザ名に割り当てられます。ユーザは、クライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。または、**smart-tunnel auto-start** コマンドを使用して、ユーザがログインしたときに自動的にスマート トンネル アクセスを開始できます。

いずれのコマンドでも、**smart-tunnel list** コマンドを使用して、最初にアプリケーションのリストを作成する必要があります。

例

次のコマンドでは、apps1 という名前のスマート トンネル リストをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel enable apps1
hostname(config-group-webvpn)
```

次のコマンドでは、apps1 という名前のリストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル リストを継承します。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no smart-tunnel
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN コンフィギュレーションを、すべてのスマート トンネル リスト エントリを含めて表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel list

プライベート サイトに接続する場合にクライアントレス（ブラウザベース）SSL VPN セッションを使用できるアプリケーションのリストに入力するには、webvpn コンフィギュレーション モードで **smart-tunnel list** コマンドを使用します。

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]

アプリケーションをリストから削除するには、このコマンドの **no** 形式を使用して、エントリを指定します。アプリケーションのリスト全体をセキュリティ アプライアンス コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用して、リストだけを指定します。

no smart-tunnel list *list*

構文の説明

list	アプリケーションまたはプログラムのリストの名前。スペースを含む場合、名前の前後に引用符を使用します。コンフィギュレーション内にリストが存在しない場合は、CLI によって作成されます。存在する場合、リストにエントリを追加します。
application	スマート トンネル アクセスが付与されるアプリケーションの名前。文字列は最大 64 文字まで使用できます。
path	Mac OS の場合は、アプリケーションのフル パス。Windows の場合は、アプリケーションのファイル名。または、ファイル名を含むアプリケーションのフル パスまたは部分パス。ストリングには最大 128 文字を使用できます。
platform *OS*	（OS が Microsoft Windows の場合は任意）**windows** または **mac** を入力して、アプリケーションのホストを指定します。
hash	（任意。Windows にのみ該当）この値を取得するには、アプリケーションのチェックサム（つまり、実行ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュを計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft File Checksum Integrity Verifier（FCIV; ファイル チェックサム整合性検証）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。FCIV のインストール後、スペースを含まないパス（c:/fciv.exe など）に、ハッシュするアプリケーションの一時コピーを置き、コマンドラインで **fciv.exe -sha1** *application* と入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。 SHA-1 ハッシュは、常に 16 進数 40 文字です。

デフォルト

Windows がデフォルトのプラットフォームです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	**platform** *OS* が追加されました。

使用上のガイドライン

複数のスマート トンネル リストをセキュリティ アプライアンスで設定できますが、複数のスマート トンネル リストを特定のグループ ポリシーまたはユーザ名に割り当てることはできません。スマート トンネル リストに入力するには、アプリケーションごとに **smart-tunnel list** コマンドを 1 回入力します。同じ *list* ストリングを入力しますが、OS で一意の *application* および *path* を指定します。リストでサポートする各 *OS* について、コマンドを 1 回入力します。

OS がエントリで指定されたものと一致しない場合、セッションでリスト エントリは無視されます。アプリケーションのパスが存在しない場合も、エントリは無視されます。

SSL VPN コンフィギュレーション内のスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。

path はコンピュータ上のものと一致する必要がありますが、完全である必要はありません。たとえば、実行ファイルとその拡張子だけで *path* を構成できます。

スマート トンネルには次の要件があります。

- スマート トンネル接続を開始するリモート ホストでは、32 ビット バージョンの Microsoft Windows Vista、Windows XP、または Windows 2000、あるいは Mac OS 10.4 または 10.5 が実行されている必要があります。
- スマート トンネルまたはポート フォワーディングを使用する Microsoft Windows Vista のユーザは、ASA の URL を [Trusted Site] ゾーンに追加する必要があります。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動して、[Tools] > [Internet Options] > [Security] タブを選択する必要があります。Vista ユーザは、[Protected Mode] をディセーブルにしてスマート トンネル アクセスを容易にすることもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法は推奨しません。
- ブラウザで Java、Microsoft ActiveX、またはその両方をイネーブルにする必要があります。
- Mac OS のスマート トンネル サポートには、Safari 3.1.1 以降が必要です。

Microsoft Windows では、Winsock 2、TCP ベースのアプリケーションのみがスマート トンネル アクセスに適格です。

Mac OS では、SSL ライブラリにダイナミックにリンクされた、TCP を使用するアプリケーションをスマート トンネルで使用できます。次のタイプのアプリケーションは、スマート トンネルで使用できません。

- dlopen または dlsym を使用して libsocket コールを特定するアプリケーション
- libsocket コールを特定するためにスタティックにリンクされたアプリケーション
- 2 レベルのネーム スペースを使用する Mac OS アプリケーション
- Mac OS のコンソールベースのアプリケーション（Telnet、SSH、cURL など）
- PowerPC MAC オペレーティング システムはスマート トンネルではサポートされません。

Mac OS では、ポータル ページから起動されたアプリケーションだけがスマート トンネル セッションを確立できます。この要件には、Firefox のスマート トンネル サポートが含まれています。スマート トンネルの最初の使用中に Firefox を使用して Firefox の別のインスタンスを起動するには、csco_st という名前のユーザ プロファイルが必要です。このユーザ プロファイルが存在しない場合、セッションでは、作成するようにユーザに要求します。

次の制限事項がスマート トンネルに適用されます。

- リモート コンピュータがセキュリティ アプライアンスにアクセスするためにプロキシ サーバを必要とする場合、接続の終端側の URL が、プロキシ サービスから除外される URL のリストに存在する必要があります。この設定では、スマート トンネルは基本認証だけをサポートします。
- セキュリティ アプライアンスは Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。スマート トンネル機能もポート フォワーディングも MAPI をサポートしていません。MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモート ユーザが AnyConnect を使用する必要があります。
- スマート トンネル自動サインオン機能では、Microsoft Windows OS 上の Microsoft WININET ライブラリを使用して HTTP または HTTPS 通信を行うアプリケーションのみがサポートされます。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。
- グループ ポリシーまたはローカル ユーザ ポリシーでは、スマート トンネル アクセスに適格なアプリケーションのリスト 1 つと、スマート トンネル自動サインオン サーバのリスト 1 つだけがサポートされます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されません。ユーザはフェールオーバー後に再接続する必要があります。

（注） スマート トンネル アクセスで突然問題が発生した場合、アプリケーションのアップグレードにより、*path* 値が最新でないことを示している場合があります。たとえば、アプリケーションおよび次のアップグレードを作成する会社が買収されると、アプリケーションのデフォルトのパスは通常は変更されます。

ハッシュを入力すると、*path* で指定したストリングと一致する不適格なファイルがクライアントレス SSL VPN によって認定されないことが、ある程度保証されます。チェックサムはアプリケーションの各バージョンまたはパッチによって異なるため、入力する *hash* が一致するのは、リモート ホスト上の 1 つのバージョンまたはパッチのみです。アプリケーションの複数のバージョンに対して *hash* を指定するには、各バージョンに対して **smart-tunnel list** コマンドを 1 回入力します。このとき、各コマンドでは、同じ *list* ストリングを入力しますが、一意の *application* ストリングと一意の *hash* 値を指定します。

（注） *hash* 値を入力し、スマート トンネル アクセスでアプリケーションの今後のバージョンまたはパッチをサポートする場合は、今後もスマート トンネル リストを維持する必要があります。スマート トンネル アクセスで突然問題が発生した場合、アプリケーションのアップグレードにより、*hash* 値を含むアプリケーション リストが最新でないことを示している場合があります。この問題は *hash* を入力しないことによって回避できます。

スマート トンネル リストのコンフィギュレーションに続き、**smart-tunnel auto-start** または **smart-tunnel enable** コマンドを使用して、グループ ポリシーまたはユーザ名にリストを割り当てます。

例

次のコマンドでは、connect.exe という名前の Microsoft Windows アプリケーションを apps1 という名前のスマート トンネル リストに追加します。

```
hostname(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

次のコマンドでは、Windows アプリケーション msimn.exe を追加し、リモート ホスト上のアプリケーションのハッシュが、スマート トンネル アクセスを許可するために入力された最後のストリングと一致することを要求します。

```
hostname(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

次のコマンドでは、Mac OS ブラウザ Safari にスマート トンネル サポートを提供します。

```
hostname(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform mac
```

関連コマンド

コマンド	説明
show running-config webvpn smart-tunnel	セキュリティ アプライアンスのスマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。

smartcard-removal-disconnect

スマート カードがユーザのコンピュータから取り外された場合に IPSec クライアント セッションを切断または保持するには、グループ ポリシー コンフィギュレーション モードで **smartcard-removal-disconnect** コマンドを使用します。

smartcard-removal-disconnect {**enable** | **disable**}

グループ ポリシーから **smartcard-removal-disconnect** コマンドを削除し、デフォルトのグループ ポリシーから設定を継承するには、このコマンドの **no** 形式を使用します。

no smartcard-removal-disconnect

構文の説明

enable	スマート カードがユーザのコンピュータから取り外された場合に IPSec クライアント セッションを終了します。
disable	スマート カードがユーザのコンピュータから取り外されても IPSec クライアント セッションを続行します。

デフォルト

enable

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、認証に使用されるスマート カードが取り外された場合に IPSec クライアント セッションは切断されます。接続中にスマート カードをコンピュータに入れたままにする必要がないようにする場合は、**smartcard-removal-disconnect disable** コマンドを入力します。

例

次のコマンドでは、スマート カードがユーザのコンピュータから取り外されてもクライアント セッションが続行するようにします。

```
hostname(config-group-policy)# smartcard-removal-disconnect disable
hostname(config-group-policy)
```

次のコマンドでは、スマート カードがユーザのコンピュータから取り外された場合にクライアント セッションが終了されるようにします。

```
hostname(config-group-policy)# smartcard-removal-disconnect enable
```

smtp from-address

ローカル CA サーバが生成するすべての電子メール（ワンタイム パスワードの配布など）の送信者フィールドで使用する電子メール アドレスを指定するには、CA サーバ コンフィギュレーション モードで **smtp from-address** コマンドを使用します。電子メール アドレスをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

smtp from-address *e-mail_address*

no smtp from-address

構文の説明

e-mail_address	CA サーバが生成するすべての電子メールの送信者フィールドに表示する電子メール アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、ローカル CA サーバからの、すべての電子メールの送信者フィールドに ca-admin@asa1-ca.example.com が含まれるように指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp from-address ca-admin@asa1-ca.example.com
hostname(config-ca-server)#
```

次に、ローカル CA サーバからの、すべての電子メールの送信者フィールドをデフォルトのアドレス admin@asa1-ca.example.com にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp from-address admin@asa1-ca.example.com
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示するテキストをカスタマイズします。

smtp subject

ローカル Certificate Authority（CA; 認証局）サーバが生成するすべての電子メール（ワンタイム パスワードの配布など）の件名フィールドに表示するテキストをカスタマイズするには、CA サーバ コンフィギュレーション モードで **smtp subject** コマンドを使用します。テキストをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

smtp subject *subject-line*

no smtp subject

構文の説明

subject-line	CA サーバから送信するすべての電子メールの件名フィールドに表示するテキストを指定します。最大文字数は 127 です。

デフォルト

デフォルトでは、件名フィールドのテキストは「Certificate Enrollment Invitation」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、CA サーバからの、すべての電子メールの件名フィールドにテキスト *Action: Enroll for a certificate* を表示するように指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp subject Action: Enroll for a certificate
hostname(config-ca-server)#
```

次に、CA サーバからの、すべての電子メールの件名フィールドのテキストをデフォルトのテキスト「Certificate Enrollment Invitation」にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no smtp subject
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
smtp from-address	ローカル CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。

smtps

SMTPS コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **smtps** コマンドを使用します。SMTPS コマンド モードで入力されたコマンドを削除するには、このコマンドの **no** 形式を使用します。SMTPS は、SSL 接続での電子メールの送信を可能にする TCP/IP プロトコルです。

smtps

no smtps

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、SMTPS コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# smtps
hostname(config-smtps)#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
show running-config smtps	SMTPS の実行コンフィギュレーションを表示します。

smtp-server

SMTP サーバを設定するには、グローバル コンフィギュレーション モードで **smtp-server** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。

セキュリティ アプライアンスには、内部 SMTP クライアントが含まれており、特定のイベントが発生したことを外部エンティティに通知するためにイベント システムで使用できます。これらのイベント通知を受信し、指定された電子メール アドレスに転送するように SMTP サーバを設定できます。SMTP 機能がアクティブになるのは、セキュリティ アプライアンス で電子メール イベントがイネーブルな場合だけです。

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

構文の説明

primary_server	プライマリ SMTP サーバを指定します。IP アドレスまたは DNS 名を使用します。
backup_server	プライマリ SMTP サーバを使用できない場合にイベント メッセージをリレーするバックアップ SMTP サーバを識別します。IP アドレスまたは DNS 名を使用します。

デフォルト

デフォルトでは、SMTP サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、SMTP サーバを IP アドレス 10.1.1.24 を使用して設定し、バックアップ SMTP サーバを IP アドレス 10.1.1.34 を使用して設定する例を示します。

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp-map

SNMP インスペクションのパラメータを定義するための特定のマップを指定するには、グローバル コンフィギュレーション モードで **snmp-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

snmp-map *map_name*

no snmp-map *map_name*

構文の説明

map_name	SNMP マップ名です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

snmp-map コマンドを使用して、SNMP インスペクションのパラメータを定義するために使用する特定のマップを指定します。このコマンドを入力すると、SNMP マップ コンフィギュレーション モードが開始され、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。SNMP マップの定義後、**inspect snmp** コマンドを使用してマップをイネーブルにします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、**inspect** コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

例

次に、SNMP トラフィックを指定し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する例を示します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
```

```
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

snmp-server community

SNMP コミュニティ ストリングを設定するには、グローバル コンフィギュレーション モードで **snmp-server community** コマンドを使用します。コミュニティ ストリングを削除するには、このコマンドの **no** 形式を使用します。

snmp-server community *text*

no snmp-server community [*text*]

構文の説明

text	コミュニティ ストリングを設定します。

デフォルト

コミュニティ ストリングは **public** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理されるネットワーク ノード間の共有秘密です。セキュリティ アプライアンスは、キーを使用して、着信 SNMP 要求が有効であるかどうかを判断します。たとえば、サイトにコミュニティ ストリングを指定してから、ルータ、セキュリティ アプライアンス、および管理ステーションに同じストリングを設定できます。セキュリティ アプライアンスはこのストリングを使用し、無効なコミュニティ ストリングを持つ要求には応答しません。

例

次の例では、コミュニティ ストリングを wallawallabingbang に設定します。

```
hostname(config)# snmp-server community wallawallabingbang
```

関連コマンド

コマンド	説明
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server contact

SNMP サーバのコンタクト名を設定するには、グローバル コンフィギュレーション モードで **snmp-server contact** コマンドを使用します。SNMP のコンタクト名を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *text*

no snmp-server contact [*text*]

構文の説明

text	コンタクト担当者またはセキュリティ アプライアンス システム管理者の名前を指定します。名前は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例では、SNMP サーバの連絡先を Pat Johnson と設定します。

```
hostname(config)# snmp-server contact Pat Johnson
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable

セキュリティ アプライアンスで SNMP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable** コマンドを使用します。SNMP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable

no snmp-server enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

SNMP サーバはイネーブルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、SNMP トラップやその他の設定を行ったり、これらを再設定しなくても、SNMP を簡単にイネーブルまたはディセーブルにすることができます。

例

次の例では、SNMP をイネーブルにし、SNMP のホストとトラップを設定してから、トラップをシステム メッセージとして送信しています。

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。

コマンド	説明
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable traps

セキュリティ アプライアンスの NMS へのトラップ送信をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。トラップをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

構文の説明

all	すべてのトラップをイネーブルにします。
entity [*trap*]	エンティティ トラップをイネーブルにします。**entity** のトラップは次のとおりです。 • **config-change** • **fru-insert** • **fru-remove**
ipsec [*trap*]	IPSec トラップをイネーブルにします。**ipsec** のトラップは次のとおりです。 • **start** • **stop**
remote-access [*trap*]	リモート アクセス トラップをイネーブルにします。リモート アクセスのトラップは次のとおりです。 • **session-threshold-exceeded**
snmp [*trap*]	SNMP トラップを有効にします。デフォルトでは、すべての SNMP トラップはイネーブルになっています。**snmp** のトラップは次のとおりです。 • **authentication** • **linkup** • **linkdown** • **coldstart**
syslog	システム ログ メッセージのトラップをイネーブルにします。

デフォルト

デフォルトのコンフィギュレーションでは、すべての **snmp** トラップがイネーブルです（**snmp-server enable traps snmp authentication linkup linkdown coldstart**）。これらのトラップをディセーブルにするには、**snmp** キーワードを指定してこのコマンドの **no** 形式を使用します。ただし、**clear configure snmp-server** コマンドを使用すると、SNMP トラップのデフォルトのイネーブル状態に戻ります。

このコマンドを入力し、トラップ タイプを指定しない場合、デフォルトは **syslog** です（デフォルトの **snmp** トラップは **syslog** トラップとともに引き続きイネーブルのままです）。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　機能タイプごとにこのコマンドを入力して、個々のトラップまたはトラップのセットをイネーブルにするか、**all** キーワードを入力してすべてのトラップをイネーブルにします。

NMS にトラップを送信するには、**logging history** コマンドを入力し、**logging enable** コマンドを使用してロギングをイネーブルにします。

例　次の例では、SNMP をイネーブルにし、SNMP のホストとトラップを設定してから、トラップをシステム メッセージとして送信しています。

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server group

新しい SNMP グループを設定するには、グローバル コンフィギュレーション モードで **snmp-server group** コマンドを使用します。指定した SNMP グループを削除するには、このコマンドの **no** 形式を使用します。

snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

no snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

構文の説明

auth	暗号化を使用しないパケット認証を指定します。
group-name	グループの名前を指定します。
noauth	パケット認証を指定しません。
priv	暗号化されたパケット認証を指定します。
v3	グループが SNMP バージョン 3 セキュリティ モデルを使用することを指定します。このセキュリティ モデルは、サポートされているものの中で最もセキュアです。このバージョンでは、認証特性を明示的に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが導入されました。

使用上のガイドライン

バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定した後、SNMP ホストを設定する必要があります。バージョン 3 およびセキュリティ レベルも指定する必要があります。コミュニティ ストリングが内部的に設定されている場合、「public」という名前の 2 つのグループが自動的に作成されます。1 つはバージョン 1 セキュリティ モデル用、もう 1 つはバージョン 2c セキュリティ モデル用です。コミュニティ ストリングを削除すると、設定された両方のグループが自動的に削除されます。

（注） 特定のグループに属すように設定されるユーザは、グループと同じセキュリティ モデルを持つ必要があります。

例

次の例に、セキュリティ アプライアンスが SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する方法について示します。これには、グループ、ユーザ、ホストの作成が含まれます。

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP コンフィギュレーション カウンタをクリアします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server user	新しい SNMP ユーザを作成します。

snmp-server host

セキュリティ アプライアンスで SNMP を使用可能な NMS を指定するには、グローバル コンフィギュレーション モードで **snmp-server host** コマンドを使用します。NMS をディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

no snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

構文の説明

0	（任意）暗号化されていない（クリア テキストの）コミュニティ ストリングが続くことを指定します。
8	暗号化されたコミュニティ ストリングが続くことを指定します。
community	NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。SNMP バージョン 1 または 2c でのみ有効です。
community-string	通知とともに、または NMS からの要求内で送信される、パスワードに似たコミュニティ ストリングを指定します。このコミュニティ ストリングは最大 32 文字です。暗号化フォーマットと非暗号化フォーマット（クリア テキスト）を使用できます。
hostname	SNMP 通知ホストを指定します。通常は NMS または SNMP マネージャです。
interface	NMS がセキュリティ アプライアンスとの通信に使用するインターフェイス名を指定します。
ip_address	SNMP トラップの送信先または SNMP 要求の送信元の NMS の IP アドレスを指定します。IPv4 アドレスのみをサポートしています。
poll	（任意）ホストはブラウズ（ポーリング）は可能だが、トラップは送信されないことを指定します。
port	NMS ホストの UDP ポート番号を設定します。
trap	（任意）トラップの送信のみが可能であり、このホストはブラウズ（ポーリング）できないことを指定します。
udp-port	（任意）SNMP トラップはデフォルト以外のポートで NMS ホストに送信される必要があることを指定します。
version {**1** | **2c** | **3**}	（任意）トラップの送信に使用する SNMP 通知バージョンを、バージョン 1、2c、または 3 に設定します。

デフォルト

デフォルトの UDP ポートは 162 です。

デフォルトのバージョンは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(5)	暗号化パスワードのサポートが追加されました。

使用上のガイドライン

最大 32 個の NMS を指定できます。現在使用中のポートで **snmp-server host** コマンドを設定すると、次のメッセージが表示されます。

警告　**The UDP port *port* is in use by another feature.SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

例

バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定し、SNMP ホストを設定する必要があります。ユーザ名はデバイス上で設定済みである必要があります。デバイスがフェールオーバー ペアのスタンバイ ユニットとして設定される場合、SNMP エンジン ID とユーザ コンフィギュレーションはアクティブ ユニットから複製されます。このアクションによって、SNMP バージョン 3 クエリーの観点から、トランスペアレントなスイッチオーバーが可能になります。スイッチオーバー イベントに対応するために NMS でのコンフィギュレーション変更は必要ありません。

暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。

暗号化されたコミュニティ ストリングは常にセキュリティ アプライアンスによって生成されます。通常は、クリア テキストの形式で入力します。

セキュリティ アプライアンスの起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

（注）　セキュリティ アプライアンス ソフトウェアをバージョン 8.0(5) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリア テキストに戻してから結果を保存する必要があります。

次に、境界インターフェイスに接続された 10.1.2.42 をホストに設定する例を示します。

```
hostname(config)# snmp-server host perimeter 10.1.2.42
```

次の例に､セキュリティ アプライアンスが SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する方法について示します。これには、グループ、ユーザ、ホストの作成が含まれます。

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

次に、暗号化されたコミュニティ ストリングを使用するようにホストを設定する例を示します。

```
hostname(config)# snmp-server host mgmt 1.2.3.4 community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

次に、暗号化されていないコミュニティ ストリングを使用するようにホストを設定する例を示します。

```
hostname(config)# snmp-server host mgmt 1.2.3.4 community 0 cisco
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server listen-port

SNMP 要求のリスニング ポートを設定するには、グローバル コンフィギュレーション モードで **snmp-server listen-port** コマンドを使用します。デフォルトのポートに戻すには、このコマンドの **no** 形式を使用します。

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

構文の説明

lport	着信要求が受け入れられるポート。デフォルト ポートは 161 です[1]。

1. **snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。

デフォルト

デフォルト ポートは 161 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

警告　**The UDP port *port* is in use by another feature.SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

例

次に、リスニング ポートを 192 に設定する例を示します。

```
hostname(config)# snmp-server listen-port 192
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server location

SNMP のセキュリティ アプライアンスの場所を設定するには、グローバル コンフィギュレーション モードで **snmp-server location** コマンドを使用します。場所を削除するには、このコマンドの **no** 形式を使用します。

snmp-server location *text*

no snmp-server location [*text*]

構文の説明

location *text*	セキュリティ アプライアンスの場所を指定します。**location** *text* は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、SNMP のセキュリティ アプライアンスの場所を Building 42、Sector 54 として設定する例を示します。

```
hostname(config)# snmp-server location Building 42, Sector 54
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。

snmp-server user

新しい SNMP ユーザを設定するには、グローバル コンフィギュレーション モードで **snmp-server user** コマンドを使用します。指定した SNMP ユーザを削除するには、このコマンドの **no** 形式を使用します。

snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

no snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

構文の説明

128	（任意）暗号化について 128 ビット AES アルゴリズムの使用を指定します。
192	（任意）暗号化について 192 ビット AES アルゴリズムの使用を指定します。
256	（任意）暗号化について 256 ビット AES アルゴリズムの使用を指定します。
3des	（任意）暗号化について 168 ビット 3DES アルゴリズムの使用を指定します。
aes	（任意）暗号化について AES アルゴリズムの使用を指定します。
auth	（任意）使用する認証レベルを指定します。
auth-password	（任意）エージェントがホストからパケットを受信できるようにするストリングを指定します。最小の長さは 1 文字、最低 8 文字で英文字と数字を含むものを推奨します。最大長は、64 文字です。プレーン テキストのパスワードか、ローカライズされた MD5 ダイジェストを指定できます。ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイジェストは、aa:bb:cc:dd という形式であることが必要です（aa、bb、cc は 16 進数の値）。ダイジェストは正確に 16 個のオクテットであることが必要です。
des	（任意）暗号化について 56 ビット DES アルゴリズムの使用を指定します。
encrypted	（任意）パスワードが暗号化された形式で表示されるかどうかを指定します。暗号化されたパスワードは、16 進数の形式である必要があります。
group-name	ユーザが属すグループの名前を指定します。
md5	（任意）HMAC-MD5-96 認証レベルを指定します。
priv	暗号化されたパケット認証を指定します。
priv-password	（任意）プライバシー ユーザ パスワードを示すストリングを指定します。最小の長さは 1 文字、最低 8 文字で英文字と数字を含むものを推奨します。最大長は、64 文字です。プレーン テキストのパスワードか、ローカライズされた MD5 ダイジェストを指定できます。ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイジェストは、aa:bb:cc:dd という形式であることが必要です（aa、bb、cc は 16 進数の値）。ダイジェストは正確に 16 個のオクテットであることが必要です。
sha	（任意）HMAC-SHA-96 認証レベルを指定します。
username	エージェントに接続するホストのユーザ名を指定します。
v3	SNMP バージョン 3 セキュリティ モデルを使用することを指定します。**encrypted**、**priv**、または **auth** キーワードの使用を許可します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが導入されました。

使用上のガイドライン　SNMP ユーザは、SNMP グループの一部である必要があります。バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定した後、SNMP ホストを設定する必要があります。

（注）　パスワードを忘れた場合は、回復できないため、ユーザを再設定する必要があります。

snmp-server user のコンフィギュレーションがコンソールに表示されるか、ファイル（スタートアップ コンフィギュレーション ファイルなど）に書き込まれる場合、ローカライズされた認証およびプライバシー ダイジェストが常にプレーン テキストのパスワードの代わりに表示されます。この使用法は、RFC 3414、11.2 項によって要求されています。

（注）　3DES または AES アルゴリズムを使用してユーザを設定するには、3DES または AES 機能のライセンスが必要です。

セキュリティ アプライアンスの起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

例　次に、セキュリティ アプライアンスで SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する例を示します。

```
hostname(config)# snmp-server group engineering v3 auth
hostname(config)# snmp-server user engineering v3 auth sha mypassword
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server group	新しい SNMP グループを作成します。
snmp-server host	SNMP ホスト アドレスを設定します。

software-version

サーバまたはエンドポイントのソフトウェア バージョンを表示するサーバおよびユーザ エージェント ヘッダー フィールドを識別するには、パラメータ コンフィギュレーション モードで **software-version** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

software-version action {**mask** | **log**} [**log**}

no software-version action {**mask** | **log**} [**log**}

構文の説明

mask	SIP メッセージ内のソフトウェア バージョンをマスクします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップでソフトウェア バージョンを識別する例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# software-version action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
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。

speed

銅線（RJ-45）イーサネット インターフェイスの速度を設定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。速度設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

no speed [**auto** | **10** | **100** | **1000** | **nonegotiate**]

構文の説明

10	速度を 10BASE-T に設定します。
100	速度を 100BASE-T に設定します。
1000	速度を 1000BASE-T に設定します。銅線ギガビット イーサネットの場合のみ。
auto	速度を自動検出します。
nonegotiate	ファイバ インターフェイスの場合は、速度を 1000 Mbps に設定し、リンク パラメータをネゴシエートしません。ファイバ インターフェイスに対して使用できる設定は、このコマンドとこのコマンドの **no** 形式だけです。値を **no speed nonegotiate**（デフォルト）に設定すると、インターフェイスでリンク ネゴシエーションがイネーブルになり、フロー制御パラメータとリモート障害情報が交換されます。

デフォルト

銅線インターフェイスの場合、デフォルトは **speed auto** です。

ファイバ インターフェイスの場合、デフォルトは **no speed nonegotiate** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

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

使用上のガイドライン

速度は物理インターフェイスだけで設定します。

ネットワークで自動検出がサポートされていない場合は、速度を特定の値に設定します。

ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行す

ることでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

PoE ポートで速度を **auto** 以外に設定する場合（可能な場合）、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコ ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

例

次に、速度を 1000BASE-T に設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
duplex	デュプレックス モードを設定します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイス コンフィギュレーションを表示します。

split-dns

スプリット トンネルを介して解決されるドメインのリストを入力するには、グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ドメインのリストをすべて削除するには、**no split-dns** コマンドを引数なしで使用します。これにより、**split-dns none** コマンドを発行して作成されたヌル リストを含め、設定されているスプリット トンネリング ドメインのリストはすべて削除されます。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルトのグループ ポリシー内に存在するリストを継承します。このようなスプリット トンネリング ドメインのリストをユーザが継承しないようにするには、**split-dns none** コマンドを使用します。

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

構文の説明

value *domain-name*	スプリット トンネルを介してセキュリティ アプライアンスが解決するドメイン名を指定します。
none	スプリット DNS リストがないことを指定します。スプリット DNS リストをヌル値で設定して、スプリット DNS リストを拒否します。デフォルトのグループ ポリシーまたは指定したグループ ポリシーのスプリット DNS リストを継承しません。

デフォルト

スプリット DNS はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ドメインのリスト内の各エントリを区切るには、単一のスペースを使用します。エントリ数に制限はありませんが、ストリング全体の長さは 255 文字以下にします。英数字、ハイフン（-）、およびピリオド（.）のみを使用できます。

no split-dns コマンドを引数なしで使用すると、**split-dns none** コマンドを発行して作成したヌル値を含め、現在の値はすべて削除されます。

AnyConnect VPN Client と SSL VPN Client はいずれもスプリット DNS をサポートしていません。

例

次に、FirstGroup という名前のグループ ポリシーに対してスプリット トンネリングを介して解決されるドメイン Domain1、Domain2、Domain3、および Domain4 を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドの除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。
split-tunnel-policy	IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

split-horizon

EIGRP スプリット ホライズンを再度イネーブルにするには、インターフェイス コンフィギュレーション モードで **split-horizon** コマンドを使用します。EIGRP スプリット ホライズンをディセーブルにするには、このコマンドの **no** 形式を使用します。

split-horizon eigrp *as-number*

no split-horizon eigrp *as-number*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。

デフォルト

split-horizon コマンドはイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

X.25 パケットスイッチド ネットワーク上のリンクを含むネットワークでは、**neighbor** コマンドを使用してスプリット ホライズン機能を無効にすることができます。代わりに、コンフィギュレーションで **no split-horizon eigrp** コマンドを明示的に指定することもできます。ただし、その場合、そのネットワーク上の関連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバに対して、同様にスプリット ホライズンをディセーブルにする必要があります。

通常、スプリット ホライズンのデフォルトの状態は、ルートを適切にアドバタイズするために変更することがアプリケーションにおいて必要となる場合を除き、変更しないことを推奨します。シリアル インターフェイスでスプリット ホライズンがディセーブルであり、そのインターフェイスがパケットスイッチド ネットワークに接続されている場合、そのネットワーク上の関連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバに対して、スプリット ホライズンをディセーブルにする必要があります。

例

次に、インターフェイス Ethernet0/0 で EIGRP スプリット ホライズンをディセーブルにする例を示します。

```
hostname(config)# interface Ethernet0/0
hostname(config-if)# no split-horizon eigrp 100
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

split-tunnel-network-list

スプリット トンネリングのネットワーク リストを作成するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用します。ネットワーク リストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ネットワーク リストをすべて削除するには、**no split-tunnel-network-list** コマンドを引数なしで使用します。これにより、**split-tunnel-network-list none** コマンドを発行して作成されたヌル リストを含め、設定されているネットワーク リストはすべて削除されます。

スプリット トンネリング ネットワーク リストがない場合、ユーザはデフォルトのグループ ポリシーまたは指定したグループ ポリシー内に存在するネットワーク リストを継承します。このようなネットワーク リストをユーザが継承しないようにするには、**split-tunnel-network-list none** コマンドを使用します。

スプリット トンネリング ネットワーク リストによって、トラフィックがトンネルを通過する必要があるネットワークと、トンネリングを必要としないネットワークが区別されます。

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

構文の説明

value *access-list name*	トンネリングするネットワークまたはトンネリングしないネットワークを列挙するアクセス リストを指定します。
none	スプリット トンネリングのネットワーク リストがないことを指定します。セキュリティ アプライアンスによって、すべてのトラフィックがトンネリングされます。 スプリット トンネリング ネットワーク リストをヌル値で設定して、スプリット トンネリングを拒否します。デフォルトのグループ ポリシーまたは指定したグループ ポリシーのデフォルトのスプリット トンネリング ネットワーク リストを継承しません。

デフォルト

デフォルトでは、スプリット トンネリング ネットワーク リストはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、ネットワーク リストに基づいてスプリット トンネリングの判断が行われます。ネットワーク リストは、プライベート ネットワーク上のアドレスのリストで構成される標準 ACL です。

no split-tunnel-network-list コマンドを引数なしで使用すると、**split-tunnel-network-list none** コマンドを発行して作成したヌル値を含め、現在のネットワーク リストはすべて削除されます。

例

次に、FirstGroup という名前のグループ ポリシーに対して FirstList という名前のネットワーク リストを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
default-domain	ドメイン フィールドの除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-policy	IPSec クライアントが条件に応じてパケットを暗号化形式で IPSec トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようにします。

split-tunnel-policy

スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを使用します。実行コンフィギュレーションから split-tunnel-policy 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーのスプリット トンネリングの値を継承できます。

スプリット トンネリングを使用すると、リモート アクセス IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようになります。スプリット トンネリングをイネーブルにすると、宛先が IPSec トンネルの反対側ではないパケットでは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングは必要なくなります。

このコマンドでは、このスプリット トンネリング ポリシーが特定のネットワークに適用されます。

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

構文の説明

excludespecified	トラフィックを暗号化しないで送信する先となるネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザにとって役立ちます。このオプションは、Cisco VPN Client だけに適用されます。
split-tunnel-policy	トラフィックのトンネリングのルールを設定することを指定します。
tunnelall	トラフィックを暗号化しないで送信しないこと、またはセキュリティ アプライアンス以外の宛先に送信しないことを指定します。リモート ユーザは、インターネット ネットワークに社内ネットワークを介してアクセスし、ローカル ネットワークにはアクセスできません。
tunnelspecified	指定したネットワークから、または指定したネットワークへのすべてのトラフィックをトンネリングします。このオプションによって、スプリット トンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。その他のすべてのアドレスへのデータは暗号化しないで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

デフォルト

スプリット トンネリングは、デフォルト（tunnelall）ではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

スプリット トンネリングは、本来は、セキュリティ機能ではなくトラフィック管理機能です。最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドの除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list none	スプリット トンネリングのアクセス リストがないことを指定します。トラフィックはすべてトンネルを通過します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。

spoof-server

HTTP プロトコル インスペクションのために、サーバ ヘッダー フィールドをストリングに置き換えるには、パラメータ コンフィギュレーション モードで **spoof-server** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

spoof-server *string*

no spoof-server *string*

構文の説明

string	サーバ ヘッダー フィールドを置き換えるストリング。最大 82 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN ストリームは **spoof-server** コマンドの対象になりません。

例

次に、HTTP インスペクション ポリシー マップでサーバ ヘッダー フィールドをあるストリングに置き換える例を示します。

```
hostname(config-pmap-p)# spoof-server string
```

関連コマンド

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

sq-period

NAC フレームワーク セッションで正常に完了したポスチャ検証と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **sq-period** コマンドを使用します。このコマンドを NAC ポリシーから削除するには、このコマンドの **no** 形式を使用します。

sq-period *seconds*

no sq-period [*seconds*]

構文の説明

seconds	正常に完了した各ポスチャ確認の間隔の秒数。指定できる範囲は 30 ～ 1800 です。

デフォルト

デフォルト値は 300 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、正常に実行された各ポスチャ検証とステータス クエリー応答の後に、ステータス クエリー タイマーを起動します。このタイマーが切れると、ホスト ポスチャの変化を調べるクエリー（*ステータス クエリー*と呼ばれる）がトリガーされます。

例

次に、ステータス クエリー タイマーの値を 1800 秒に変更する例を示します。

```
hostname(config-nac-policy-nac-framework)# sq-period 1800
hostname(config-nac-policy-nac-framework)
```

次に、NAC フレームワーク ポリシーからステータス クエリー タイマーを削除する例を示します。

```
hostname(config-nac-policy-nac-framework)# no sq-period
hostname(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
debug eap	NAC フレームワーク メッセージのデバッグのための拡張認証プロトコル イベントのロギングをイネーブルにします。

ssh

セキュリティ アプライアンスに SSH アクセスを追加するには、グローバル コンフィギュレーション モードで **ssh** コマンドを使用します。セキュリティ アプライアンスへの SSH アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

構文の説明

interface	SSH をイネーブルにするセキュリティ アプライアンス インターフェイス。指定しない場合、SSH は外部インターフェイスを除くすべてのインターフェイスでイネーブルになります。
ip_address	セキュリティ アプライアンスへの SSH 接続を開始することを認可されるホストまたはネットワークの IPv4 アドレス。ホストの場合は、ホスト名を入力することもできます。
ipv6_address/*prefix*	セキュリティ アプライアンスへの SSH 接続を開始することを認可されるホストまたはネットワークの IPv6 アドレスとプレフィックス。
mask	*ip_address* のネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ssh *ip_address* コマンドでは、セキュリティ アプライアンスへの SSH 接続を開始することを認可されるホストまたはネットワークを指定します。複数の ssh コマンドをコンフィギュレーションに含めることができます。このコマンドの **no** 形式によって、特定の SSH コマンドをコンフィギュレーションから削除します。すべての SSH コマンドを削除するには、**clear configure ssh** コマンドを使用します。

セキュリティ アプライアンスへの SSH の使用を開始する前に、**crypto key generate rsa** コマンドを使用してデフォルトの RSA キーを生成する必要があります。

セキュリティ アプライアンスでは、次のセキュリティ アルゴリズムと暗号がサポートされています。

- データ暗号化のための 3DES 暗号および AES 暗号

- パケットの完全性のための HMAC-SHA アルゴリズムおよび HMAC-MD5 アルゴリズム
- ホスト認証のための RSA 公開キー アルゴリズム
- キー交換のための Diffie-Hellman Group 1 アルゴリズム

次の SSH バージョン 2 機能は、セキュリティ アプライアンスでサポートされていません。

- X11 転送
- ポート フォワーディング
- SFTP サポート
- Kerberos と AFS のチケット引き渡し
- データ圧縮

例

次に、IP アドレス 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する例を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
crypto key generate rsa	アイデンティティ証明書用の RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh scopy enable	セキュリティ アプライアンスでセキュア コピー サーバをイネーブルにします。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、セキュリティ アプライアンスを制限します。

ssh disconnect

アクティブな SSH セッションを切断するには、特権 EXEC モードで **ssh disconnect** コマンドを使用します。

ssh disconnect *session_id*

構文の説明

session_id	ID 番号で指定した SSH セッションを切断します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セッション ID を指定する必要があります。切断する SSH セッションの ID を取得するには、**show ssh sessions** コマンドを使用します。

例

次に、切断される SSH セッションの例を示します。

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

関連コマンド

コマンド	説明
show ssh sessions	セキュリティ アプライアンスとのアクティブ SSH セッションに関する情報を表示します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

ssh scopy enable

セキュリティ アプライアンスで Secure Copy（SCP; セキュア コピー）をイネーブルにするには、グローバル コンフィギュレーション モードで **ssh scopy enable** コマンドを使用します。SCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh scopy enable

no ssh scopy enable

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SCP はサーバのみの実装です。SCP のための接続を受け入れて終了できますが、開始することはできません。セキュリティ アプライアンスには、次の制約事項があります。

- SCP のこの実装にはディレクトリ サポートはないため、セキュリティ アプライアンスの内部ファイルへのリモート クライアント アクセスは制限されます。
- SCP の使用時はバナー サポートはありません。
- SCP ではワイルドカードはサポートされません。
- SSH バージョン 2 接続をサポートするには、セキュリティ アプライアンスのライセンスに VPN-3DES-AES 機能が必要です。

ファイル転送を開始する前に、セキュリティ アプライアンスでは使用可能なフラッシュ メモリをチェックします。使用可能なスペースが十分ではない場合、セキュリティ アプライアンスは SCP 接続を終了します。フラッシュ メモリ内のファイルを上書きする場合でも、セキュリティ アプライアンスにコピーされるファイル用に十分な空きスペースが必要です。SCP プロセスでは、ファイルはまず一時ファイルにコピーされ、置き換えられるファイルに一時ファイルがコピーされます。コピーされるファイルと上書きされるファイルを保持する十分なスペースがフラッシュ内にない場合、セキュリティ アプライアンスは SCP 接続を終了します。

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh scopy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、セキュリティ アプライアンスを制限します。

ssh timeout

デフォルトの SSH セッション アイドル タイムアウト値を変更するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

ssh timeout *number*

no ssh timeout

構文の説明

number	SSH セッションが切断される前に非アクティブである時間を分単位で指定します。有効な値は、1 ～ 60 分です。

デフォルト

デフォルトのセッション タイムアウト値は、5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ssh timeout コマンドでは、セッションが切断される前にアイドルである時間を分単位で指定します。デフォルトの時間は、5 分です。

例

次に、IP アドレス 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続のみを受け入れるように、内部インターフェイスを設定する例を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。

コマンド	説明
show ssh sessions	セキュリティ アプライアンスとのアクティブ SSH セッションに関する情報を表示します。
ssh disconnect	アクティブな SSH セッションを切断します。

ssh version

セキュリティ アプライアンスが受け入れる SSH のバージョンを制限するには、グローバル コンフィギュレーション モードで **ssh version** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。デフォルト値では、セキュリティ アプライアンスへの SSH バージョン 1 接続と SSH バージョン 2 接続が許可されます。

ssh version {**1** | **2**}

no ssh version [**1** | **2**]

構文の説明

1	SSH バージョン 1 接続のみがサポートされることを指定します。
2	SSH バージョン 2 接続のみがサポートされることを指定します。

デフォルト

デフォルトでは、SSH バージョン 1 と SSH バージョン 2 の両方がサポートされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

1 および 2 によって、セキュリティ アプライアンスでの使用をいずれのバージョンの SSH に限定するかを指定します。このコマンドの **no** 形式を使用すると、セキュリティ アプライアンスはデフォルトの状態、つまり、互換モード（両方のバージョンが使用可能）に戻ります。

例

次の例に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続を受け入れるよう内部インターフェイスを設定する方法を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。

ssl certificate-authentication

クライアント証明書の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ssl certificate-authentication** コマンドを使用します。ssl 証明書の認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ssl certificate-authentication interface *interface-name* **port** *port-number*

no ssl certificate-authentication interface *interface-name* **port** *port-numbe***r**

構文の説明

interface-name	選択したインターフェイスの名前。inside、management、outside などです。
port-number	TCP ポート番号。1 ～ 65535 の範囲の整数です。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、廃止された http authentication-certificate コマンドに代わるものです。

例

次に、SSL 証明書認証機能を使用するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ssl certificate-authentication interface inside port 330
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。

ssl client-version

セキュリティ アプライアンスがクライアントとして動作する場合の SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl client-version** コマンドを使用します。デフォルトの **any** に戻すには、このコマンドの **no** バージョンを使用します。このコマンドを使用すると、セキュリティ アプライアンスによって送信される SSL/TLS のバージョンを限定できます。

ssl client-version [*any* | *sslv3-only* | *tlsv1-only*]

no ssl client-version

構文の説明

any	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
sslv3-only	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 のみが受け入れられます。
tlsv1-only	セキュリティ アプライアンスによって TLSv1 クライアントの hello が送信され、TLS バージョン 1 のみが受け入れられます。

デフォルト

デフォルト値は **any** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

TCP ポート フォワーディングは、WebVPN ユーザが次の SSL バージョンで接続している場合、動作しません。

SSLv3 でネゴシエート	Java がダウンロードされる
SSLv3/TLSv1 でネゴシエート	Java がダウンロードされる
TLSv1 でネゴシエート	Java がダウンロードされない
TLSv1 だけ	Java がダウンロードされない
SSLv3 だけ	Java がダウンロードされない

問題は、ポート フォワーディング アプリケーションを起動すると、JAVA ではクライアントの Hello パケットで SSLv3 のみがネゴシエートされることです。

例

次に、SSL クライアントとして動作する場合に TLSv1 のみを使用して通信するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ssl client-version tlsv1-only
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl server-version	サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl encryption

SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **ssl encryption** コマンドを使用します。このコマンドを再度発行すると、前の設定は上書きされます。アルゴリズムの使用の優先順位は、アルゴリズムの順序によって決まります。環境のニーズに合わせてアルゴリズムを追加または削除できます。デフォルト（暗号化アルゴリズムの完全なセット）に戻すには、このコマンドの **no** 形式を使用します。

ssl encryption [*3des-sha1*] [*des-sha1*] [*rc4-md5*] [*aes128-sha1*] [*aes256-sha1*] [*possibly others*]

no ssl encryption

構文の説明

3des-sha1	Secure Hash Algorithm 1 を使用するトリプル DES 暗号化を指定します。
des-sha1	Secure Hash Algorithm 1 を使用する DES 暗号化を指定します。
rc4-md5	MD5 ハッシュ関数を使用する RC4 暗号化を指定します。
aes128-sha1	Secure Hash Algorithm 1 を使用するトリプル AES 128 ビット暗号化を指定します。
aes256-sha1	Secure Hash Algorithm 1 を使用するトリプル AES 256 ビット暗号化を指定します。
possibly others	今後のリリースで暗号化アルゴリズムが追加される可能性があることを示します。

デフォルト

デフォルトでは、すべてのアルゴリズムを次の順序で使用できます。

[*ssl encryption***] [***rc4-sha1***] [***aes128-sha1***] [***aes256-sha1***] [***3des-sha1***]**

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM のライセンス タブには、設定した値ではなく、ライセンスでサポートされる暗号化の最大レベルが反映されます。

例

次に、3des-sha1 および des-sha1 暗号化アルゴリズムを使用するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ssl encryption 3des-sha1 des-sha1
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl server-version

サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl server-version** コマンドを使用します。デフォルトの any に戻すには、このコマンドの **no** バージョンを使用します。このコマンドを使用すると、セキュリティ アプライアンスによって受け入れられる SSL/TLS のバージョンを限定できます。

ssl server-version [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

no ssl server-version

構文の説明

any	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
sslv3	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 にネゴシエートされます。
sslv3-only	セキュリティ アプライアンスによって SSL バージョン 3 クライアントの hello のみが受け入れられ、SSL バージョン 3 のみが使用されます。
tlsv1	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、TLS バージョン 1 にネゴシエートされます。
tlsv1-only	セキュリティ アプライアンスによって TLSv1 クライアントの hello のみが受け入れられ、TLS バージョン 1 のみが使用されます。

デフォルト

デフォルト値は **any** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

TCP ポート フォワーディングは、WebVPN ユーザが次の SSL バージョンで接続している場合、動作しません。

SSLv3 でネゴシエート	Java がダウンロードされる
SSLv3/TLSv1 でネゴシエート	Java がダウンロードされる
TLSv1 でネゴシエート	Java がダウンロードされない

TLSv1 だけ	Java がダウンロードされない
SSLv3 だけ	Java がダウンロードされない

電子メール プロキシを設定する場合、SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。

例

次に、SSL サーバとして動作する場合に TLSv1 のみを使用して通信するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ssl server-version tlsv1-only
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl trust-point

インターフェイスの SSL 証明書を表す証明書トラストポイントを指定するには、グローバル コンフィギュレーション モードで **ssl trust-point** コマンドを *interface* 引数を指定して使用します。インターフェイスを指定しない場合は、トラストポイントが設定されていないすべてのインターフェイス用のフォールバック トラストポイントが作成されます。インターフェイスを指定しない SSL トラストポイントをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。インターフェイスを指定するエントリを削除するには、このコマンドの **no ssl trust-point {***trustpoint [interface]***}** 形式を使用します。

ssl trust-point {*trustpoint [interface]***}**

no ssl trust-point

構文の説明

interface	トラストポイントが適用されるインターフェイスの名前。インターフェイスの名前は **nameif** コマンドで指定します。
trustpoint	**crypto ca trustpoint** {*name*} コマンドで設定された CA トラストポイントの *name*。

デフォルト

デフォルトでは、トラストポイント アソシエーションはありません。セキュリティ アプライアンスでは、デフォルトの自己生成 RSA キー ペア証明書が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するときは、次のガイドラインに従ってください。

- *trustpoint* の値は、**crypto ca trustpoint {*name*}** コマンドで設定された CA トラストポイントの name である必要があります。
- *interface* の値は、あらかじめ設定されたインターフェイスの *nameif* 名である必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照する **ssl trust-point** エントリも削除されます。
- **ssl trustpoint** エントリは、インターフェイスごとに 1 つと、インターフェイスを指定しないもの 1 つを保持できます。
- 同じトラストポイントを複数のエントリで再利用できます。

次に、このコマンドの **no** 形式を使用する例を示します。

このコンフィギュレーションには、次の SSL トラストポイントが含まれています。

```
ssl trust-point tp1
ssl trust-point tp2 outside
```

次のコマンドを発行します。

no ssl trust-point

show run ssl を実行すると、次のように表示されます。

ssl trust-point tp2 outside

例

次に、内部インターフェイス用の FirstTrust という名前の ssl トラストポイントと、インターフェイスが関連付けられない DefaultTrust という名前のトラストポイントを設定する例を示します。

```
hostname(config)# ssl trust-point FirstTrust inside
hostname(config)# ssl trust-point DefaultTrust
```

次に、このコマンドの **no** 形式を使用して、インターフェイスが関連付けられていないトラストポイントを削除する例を示します。

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

次に、インターフェイスが関連付けられているトラストポイントを削除する例を示します。

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point FirstTrust inside
hostname(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl server-version	サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定します。

sso-server

セキュリティ アプライアンスのユーザ認証のために Single Sign-On（SSO; シングル サインオン）サーバを作成する場合、webvpn コンフィギュレーション モードで **sso-server** コマンドを使用します。このコマンドでは、SSO サーバ タイプを指定する必要があります。

SSO サーバを削除するには、このコマンドの **no** 形式を使用します。

sso-server *name* **type** [*siteminder* | *saml-v1.1-post*]

no sso-server *name*

（注） このコマンドは、SSO 認証用に必要です。

構文の説明

name	SSO サーバの名前を指定します。最小 4 文字、最大 31 文字です。
saml-v1.1-post	設定するセキュリティ アプライアンス SSO サーバが、SAML、バージョン 1.1、POST タイプの SSO サーバであることを指定します。
siteminder	設定するセキュリティ アプライアンス SSO サーバが、Computer Associates SiteMinder SSO サーバであることを指定します。
type	SSO サーバのタイプを指定します。使用できるタイプは、SiteMinder と SAML-V1.1-POST だけです。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**sso-server** コマンドを使用すると、SSO サーバを作成できます。

認証では、セキュリティ アプライアンスは SSO サーバへの WebVPN ユーザのプロキシとして動作します。セキュリティ アプライアンスは現在、SiteMinder SSO サーバ（以前の Netegrity SiteMinder）と SAML POST タイプの SSO サーバをサポートしています。現在、type オプションで使用できる引数は *siteminder* または *saml-V1.1-post* に限定されています。

例

次に、webvpn コンフィギュレーション モードで、「example1」という名前の SiteMinder-type の SSO サーバを作成する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example1 type siteminder
hostname(config-webvpn-sso-siteminder)#
```

次に、webvpn コンフィギュレーション モードで、「example2」という名前の SAML、バージョン 1.1、POST-type の SSO サーバを作成する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example2 type saml-v1.1-post
hostname(config-webvpn-sso-saml)#
```

関連コマンド

コマンド	説明
assertion-consumer-url	SAML-type の SSO アサーション コンシューマ サービスの URL を指定します。
issuer	SAML-type の SSO サーバのセキュリティ デバイス名を指定します。
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの運用統計情報を表示します。
test sso-server	テスト認証要求で SSO サーバをテストします。
trustpoint	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

sso-server value（グループ ポリシー webvpn）

SSO サーバをグループ ポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで使用可能な webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。

割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。

デフォルト ポリシーが継承されないようにするには、**sso-server none** コマンドを使用します。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

構文の説明

name	グループ ポリシーに割り当てる SSO サーバの名前を指定します。

デフォルト

グループに割り当てられるデフォルト ポリシーは、DfltGrpPolicy です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

グループ ポリシー webvpn モードで **sso-server value** コマンドを入力すると、SSO サーバをグループ ポリシーに割り当てることができます。

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは、現在、SiteMinder-type の SSO サーバと SAML POST-type の SSO サーバをサポートしています。

このコマンドは SSO サーバの両タイプに適用されます。

（注） SSO サーバをユーザ ポリシーに割り当てるには、同じコマンド **sso-server value** をユーザ名 webvpn コンフィギュレーション モードで入力します。

例

次に、グループ ポリシー my-sso-grp-pol を作成し、example という名前の SSO サーバに割り当てるサンプル コマンドを示します。

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
```

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
sso-server value（ユーザ名 webvpn）	SSO サーバをユーザ ポリシーに割り当てます。
web-agent-url	セキュリティ アプライアンスが、SiteMinder-type の SSO 認証を要求する SSO サーバの URL を指定します。

sso-server value（ユーザ名 webvpn）

SSO サーバをユーザ ポリシーに割り当てるには、ユーザ名コンフィギュレーション モードで使用可能な webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。

ユーザの SSO サーバ割り当てを削除するには、このコマンドの **no** 形式を使用します。

ユーザ ポリシーがグループ ポリシーから不要な SSO サーバ割り当てを継承している場合は、**sso-server none** コマンドを使用して割り当てを削除します。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

構文の説明

name	ユーザ ポリシーに割り当てる SSO サーバの名前を指定します。

デフォルト

デフォルトでは、ユーザ ポリシーはグループ ポリシーの SSO サーバ割り当てを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは、現在、SiteMinder-type の SSO サーバと SAML POST-type の SSO サーバをサポートしています。

このコマンドは SSO サーバの両タイプに適用されます。

sso-server value コマンドを入力すると、SSO サーバをユーザ ポリシーに割り当てることができます。

（注） SSO サーバをグループ ポリシーに割り当てるには、同じコマンド **sso-server value** をグループ webvpn コンフィギュレーション モードで入力します。

例

次に、my-sso-server という名前の SSO サーバを Anyuser という名前の WebVPN ユーザのユーザ ポリシーに割り当てるサンプル コマンドを示します。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
```

```
hostname(config-username-webvpn)# sso-server value my-sso-server
hostname(config-username-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
sso-server value（config-group-webvpn）	SSO サーバをグループ ポリシーに割り当てます。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

start-url

オプションの事前ログイン クッキーの取得先 URL を入力するには、AAA サーバ ホスト コンフィギュレーション モードで **start-url** コマンドを入力します。これは HTTP フォームのコマンドを使用した SSO です。

start-url *string*

（注） HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	SSO サーバの URL。URL の最大長は 1024 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用して、シングル サインオン認証要求を認証 Web サーバに送信できます。認証 Web サーバは、Set-Cookie ヘッダーをログイン ページのコンテンツとともに送信することによって、事前ログイン シーケンスを実行できます。このことは、認証 Web サーバのログイン ページにブラウザで直接接続することによって検出できます。ログイン ページがロードされるときに Web サーバによってクッキーが設定され、このクッキーがその後のログイン セッションに関連する場合、**start-url** コマンドを使用してクッキーの取得先 URL を入力する必要があります。実際のログイン シーケンスは、事前ログイン クッキー シーケンスの後で、認証 Web サーバへのフォーム送信により開始されます。

（注） **start-url** コマンドは、事前ログイン クッキー交換が存在する場合にのみ必要です。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、事前ログイン クッキーを取得するための URL https://example.com/east/Area.do?Page-Grp1 を指定する例を示します。

```
hostname(config)# aaa-server testgrp1 (inside) host example.com
hostname(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

state-checking

H.323 の状態チェックを実行するには、パラメータ コンフィギュレーション モードで **state-checking** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

state-checking [h225 | ras]

no state-checking [h225 | ras]

構文の説明

h225	H.225 の状態チェックを実行します。
ras	RAS の状態チェックを実行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 コールで RAS の状態チェックを実行する例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# state-checking ras
```

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。

static

実際の IP アドレスをマッピング先の IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換ルールを設定するには、グローバル コンフィギュレーション モードで **static** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

スタティック NAT の場合：

static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

no static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

スタティック PAT の場合：

static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

no static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

構文の説明

access-list *access_list_name*	拡張アクセス リストを使用して、実アドレスおよび宛先/送信元アドレスを指定します。この機能は、ポリシー NAT と呼ばれています。
	
	拡張アクセス リストを作成するには、**access-list extended** コマンドを使用します。アクセス リストの最初のアドレスは、実アドレスです。2 番めのアドレスは、トラフィックの発生元に応じて、送信元アドレスか宛先アドレスです。たとえば、10.1.1.1 がトラフィックを 209.165.200.224 ネットワークに送信するときに、実アドレス 10.1.1.1 をマッピング先のアドレス 192.168.1.1 に変換するには、**access-list** コマンドおよび **static** コマンドは次のようになります。
	
	`hostname(config)# access-list TEST extended ip host 10.1.1.1 209.165.200.224 255.255.255.224`
	`hostname(config)# static (inside,outside) 192.168.1.1 access-list TEST`
	
	この場合、2 番めのアドレスは宛先アドレスです。ただし、ホストがマッピング先のアドレスへの接続を開始する場合にも、同じコンフィギュレーションが使用されます。たとえば、209.165.200.224 ネットワーク上のホストが 192.168.1.1 への接続を開始する場合、アクセス リストの 2 番めのアドレスは送信元アドレスです。
	
	このアクセス リストには、**permit** ACE のみを含めます。オプションで、**eq** 演算子を使用して、アクセス リストに実際のポートと宛先ポートを指定できます。ポリシー NAT では **inactive** キーワードまたは **time-range** キーワードは考慮されません。ポリシー NAT コンフィギュレーションでは、すべての ACE はアクティブであると見なされます。
	
	変換のためのネットワークを指定すると（10.1.1.0 255.255.255.0 など）、セキュリティ アプライアンスは .0 と .255 のアドレスを変換します。これらのアドレスへのアクセスを禁止する場合は、アクセスを拒否するようにアクセス リストを設定する必要があります。

dns	（任意）このスタティックと一致する DNS 応答内の A レコード（アドレス レコード）を書き換えます。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へリライトされます。 **（注）** この機能をサポートするには、DNS インスペクションをイネーブルにする必要があります。
emb_lim	（任意）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。 **（注）** スタティック NAT を使用して適用される初期接続の制限は、指定したインターフェイス間の接続だけでなく、実際の IP アドレスへ、または実際の IP アドレスからのすべての接続に適用されます。特定のフローだけに制限を適用するには、**set connection** コマンドを参照してください。

interface	インターフェイスの IP アドレスを、マッピング アドレスとして使用します。インターフェイス アドレスを使用する必要がある場合はこのキーワードを使用しますが、アドレスは、DHCP を使用してダイナミックに割り当てられます。 **（注）** インターフェイスの IP アドレスをスタティック PAT エントリに含める場合は、実際の IP アドレスを指定する代わりに **interface** キーワードを使用する必要があります。
mapped_ifc	マッピング IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
mapped_ip	実アドレスの変換先アドレスを指定します。
mapped_port	マッピング先の TCP ポートまたは UDP ポートを指定します。リテラル名または 0 ～ 65535 の範囲の数字でポートを指定できます。 有効なポート番号は、次の Web サイトで確認できます。 http://www.iana.org/assignments/port-numbers
nailed	（任意）非対称でルーティングされたトラフィックの TCP セッションを許可します。このオプションを使用すると、状態を確立するための対応する発信接続がなくても、着信トラフィックはセキュリティ アプライアンスを通過できます。このコマンドは、**failover timeout** コマンドとともに使用します。**failover timeout** コマンドによって、システムが起動したかアクティブになった後に、ネイリングされたセッションが受け入れられる期間が指定されます。設定しない場合は、接続を再確立できません。 **（注）** **nailed** オプションを **static** コマンドに追加すると、その接続で TCP ステート トラッキングとシーケンス チェックがスキップされます。**asr-group** コマンドを使用して非対称ルーティングのサポートを設定する方が、**static** コマンドを **nailed** オプションを指定して使用するよりもセキュアであるため、非対称ルーティングのサポートを設定する方法として推奨されます。
netmask *mask*	実アドレスおよびマッピング先のアドレスのサブネット マスクを指定します。単一ホストの場合は、255.255.255.255 を使用します。マスクを入力しない場合は、IP アドレス クラスのデフォルト マスクが使用されます。ただし、例外が 1 つあります。マスキング後のホストビットが 0 以外の場合は、ホスト マスク 255.255.255.255 が使用されます。*real_ip* の代わりに **access-list** キーワードを使用する場合、アクセス リストで使用されるサブネット マスクは *mapped_ip* にも使用されます。

norandomseq	（任意）TCP ISN のランダム化保護をディセーブルにします。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。 保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。 TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。 • 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。 • セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。 • セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実アドレスを指定します。
real_port	実際の TCP ポートまたは UDP ポートを指定します。リテラル名または 0 ～ 65535 の範囲の数字でポートを指定できます。 有効なポート番号は、次の Web サイトで確認できます。 http://www.iana.org/assignments/port-numbers
tcp	スタティック PAT の場合、プロトコルを TCP として指定します。
tcp *max_conns*	ローカル ホストに許可する同時 TCP 接続の最大数を指定します（**local-host** コマンドを参照）。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 接続制限を設定するために推奨される方法は、ポリシー マップの中でクラスに接続制限を設定して、モジュラ ポリシー フレームワークを使用することです。
udp	スタティック PAT の場合、プロトコルを UDP として指定します。
udp *udp_max_conns*	（任意）ローカル ホストに許可する同時 UDP 接続の最大数を指定します（**local-host** コマンドを参照）。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 接続制限を設定するために推奨される方法は、ポリシー マップの中でクラスに接続制限を設定して、モジュラ ポリシー フレームワークを使用することです。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は 0（無制限）です。この値は、最大使用可能値です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2.(1)	NAT は、トランスペアレント ファイアウォール モードでサポートされるようになりました。

使用上のガイドライン

スタティック NAT では、実アドレスからマッピング先のアドレスへの固定変換が作成されます。ダイナミック NAT および PAT では、各ホストは、後続の変換ごとに異なるアドレスまたはポートを使用します。スタティック NAT では連続する各接続においてマッピング先のアドレスは同じであり、固定の変換ルールが存在するため、スタティック NAT では、宛先ネットワーク上のホストは変換されたホストへのトラフィックを開始できます（それを許可するアクセス リストがある場合）。

（注） スタティック ポリシー NAT の場合、変換の取り消しにおいて、**static** コマンド内の ACL は使用されません。パケット内の宛先アドレスがスタティック ルールのマッピング先のアドレスと一致する場合は、アドレスを未変換の状態に戻すのに、スタティック ルールが使用されます。

ダイナミック NAT と、スタティック NAT のアドレス範囲との主な違いは、スタティック NAT では、変換されたホストへの接続をリモート ホストが開始できるが（それを許可するアクセス リストがある場合）、ダイナミック NAT ではできないことです。また、スタティック NAT では、実アドレスと同じ数のマッピング先のアドレスが必要です。

スタティック ポリシー NAT では一致するポートの使用がサポートされていますが、NAT ではサポートされていません。

スタティック PAT はスタティック NAT と同じですが、実アドレスとマッピング先のアドレスに対してプロトコル（TCP または UDP）およびポートを指定できる点が異なります。

この機能を使用すると、複数の異なる static ステートメントで同じマッピング先のアドレスを指定できます。ただし、ステートメントごとにポートが異なる必要があります（複数のスタティック NAT ステートメントに対して同じマッピング先のアドレスを使用することはできません）。

スタティック PAT を使用しない限り、同じ 2 つのインターフェイス間の、複数の **static** コマンドで、同じ実アドレスまたはマッピング先のアドレスを使用することはできません。同じマッピングされているインターフェイスに対して、**global** コマンドでも定義されているマッピング先のアドレスを **static** コマンドで使用しないでください。

セカンダリ チャネルのアプリケーション インスペクションを必要とするアプリケーション（FTP、VoIP など）に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリ ポートを変換します。

変換のためのネットワークを指定すると（10.1.1.0 255.255.255.0 など）、セキュリティ アプライアンスは .0 と .255 のアドレスを変換します。これらのアドレスへのアクセスを禁止する場合は、アクセスを拒否するようにアクセス リストを設定する必要があります。

static コマンド ステートメントを変更または削除した後は、**clear xlate** コマンドを使用して変換をクリアします。

また、**set connection** コマンドを使用して、最大接続数、最大初期接続数、および TCP シーケンスのランダム化を設定できます。両方の方法を使用して同じトラフィックにこれらの設定を行う場合は、セキュリティ アプライアンスは低い方の制限を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

接続属性（**dns**、**norandomseq**、**nailed**、**tcp**、および **udp**）には、ホスト単位の制限があります。ポリシー NAT（アクセス リストを使用）や 3 つ以上のインターフェイスがある NAT などの場合、複数の **nat** コマンドと **static** コマンドから接続属性の値を生成できます。そのような場合、最初のパケットと一致するルールの値が、優先される値です。たとえば、次のコンフィギュレーションでは、TCP 接続制限 100 および 200 を適用できます。

```
static (inside,dmz) 192.168.1.1 192.168.1.100 tcp 100
static (inside,outside) 192.168.1.1 192.168.1.100 tcp 200
```

ホスト 192.168.1.1 からの最初のパケットが dmz インターフェイス向けである場合､その後のすべての TCP セッションで TCP 接続制限は 100 です。

例

スタティック NAT の例

たとえば、次のポリシー スタティック NAT の例は、宛先アドレスに応じて 2 つのマッピング先のアドレスに変換される単一の実アドレスを示しています。

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0 255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

次のコマンドでは、内部 IP アドレス（10.1.1.3）を外部 IP アドレス（209.165.201.12）にマッピングします。

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask 255.255.255.255
```

次のコマンドでは、外部アドレス（209.165.201.15）を内部アドレス（10.1.1.6）にマッピングします。

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask 255.255.255.255
```

次のコマンドでは、サブネット全体をスタティックにマッピングします。

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

次に、限定された数のユーザが Intel Internet Phone、CU-SeeMe、CU-SeeMe Pro、MeetingPoint、または Microsoft NetMeeting を使用して H.323 経由でコール インできるようにする例を示します。**static** コマンドでは、アドレス 209.165.201.0 ～ 209.165.201.30 をローカル アドレス 10.1.1.0 ～ 10.1.1.30 にマッピングします（209.165.201.1 が 10.1.1.1 にマッピング、209.165.201.10 が 10.1.1.10 にマッピングなど）。

```
hostname(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask 255.255.255.224
hostname(config)# access-list acl_out permit tcp any 209.165.201.0 255.255.255.224 eq h323
hostname(config)# access-group acl_out in interface outside
```

次の例は、Mail Guard をディセーブルにするために使用するコマンドを示しています。

```
hostname(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
hostname(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
hostname(config)# access-group acl_out in interface outside
hostname(config)# no fixup protocol smtp 25
```

この例では、**static** コマンドによって、外部ホストが dmz1 インターフェイス上にある 10.1.1.1 メール サーバ ホストにアクセスできるようにするグローバル アドレスを設定できます。DNS の MX レコードを 209.165.201.1 アドレスを指定するように設定し、メールがこのアドレスに送信されるようにする必要があります。**access-list** コマンドにより、外部ユーザは SMTP ポート（25）を通じてグローバル アドレスにアクセスできます。**no fixup protocol** コマンドにより、Mail Guard はディセーブルになります。

スタティック PAT の例

たとえば、10.1.3.0 ネットワーク上のホストからセキュリティ アプライアンス外のインターフェイス（10.1.2.14）に向かって開始される Telnet トラフィックの場合、次のコマンドを入力することによって、10.1.1.15 にある内部ホストにトラフィックをリダイレクトできます。

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

10.1.3.0 ネットワーク上のホストからセキュリティ アプライアンス外のインターフェイス（10.1.2.14）に向かって開始される HTTP トラフィックの場合、次のように入力することによって、10.1.1.15 にある内部ホストにトラフィックをリダイレクトできます。

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

Telnet トラフィックをセキュリティ アプライアンス外部インターフェイス（10.1.2.14）から内部ホスト 10.1.1.15 にリダイレクトするには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
```

ただし、上記の実際の Telnet サーバが接続を開始できるようにするには、変換を追加する必要があります。たとえば、その他のすべてのタイプのトラフィックを変換するには、次のコマンドを入力します。元の **static** コマンドは、Telnet からサーバへの変換を行います。一方、**nat** コマンドと **global** コマンドは、サーバからの発信接続のための PAT を指定します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

すべての内部トラフィックについて個別の変換も保持し、内部ホストが Telnet サーバとは異なるマッピング先のアドレスを使用する場合でも、Telnet サーバから開始されるトラフィックが、サーバへの Telnet トラフィックを許可する **static** ステートメントと同じマッピング先のアドレスを使用するように設定できます。Telnet サーバ専用の、より排他的な **nat** ステートメントを作成する必要があります。**nat** ステートメントは最も一致しているものが読み取られるため、より排他的な **nat** ステートメントは一般的なステートメントよりも前に一致します。次に、Telnet の **static** ステートメント、Telnet サーバから開始されるトラフィック用の、より排他的な **nat** ステートメント、および異なるマッピング先のアドレスを使用する他の内部ホスト用のステートメントの例を示します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

well-known ポート（80）を別のポート（8080）に変換するには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

関連コマンド

コマンド	説明
clear configure static	コンフィギュレーションから **static** コマンドを削除します。
clear xlate	すべての変換をクリアします。
nat	ダイナミック NAT を設定します。
show running-config static	コンフィギュレーション内のすべての **static** コマンドを表示します。
timeout conn	接続のタイムアウトを設定します。

strict-header-validation

RFC 3261 に従って、SIP メッセージのヘッダー フィールドの厳密な検証をイネーブルにするには、パラメータ コンフィギュレーション モードで **strict-header-validation** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

no strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

構文の説明

drop	検証発生時にパケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。任意のアクションと関連付けることができます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップで SIP ヘッダー フィールドの厳密な検証をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# strict-header-validation action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

strict-http

HTTP に準拠していないトラフィックの転送を許可するには、HTTP マップ コンフィギュレーション モードで **strict-http** コマンドを使用します。このモードには **http-map** コマンドを使用してアクセスできます。この機能をデフォルトの動作にリセットするには、このコマンドの **no** 形式を使用します。

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
log	（任意）syslog を生成します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信して接続を閉じます。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

厳密な HTTP インスペクションをディセーブルにすることはできませんが、**strict-http action allow** コマンドを使用すると、HTTP に準拠していないトラフィックの転送がセキュリティ アプライアンスで許可されます。このコマンドによって、デフォルトの動作（HTTP に準拠していないトラフィックの転送を拒否する）が上書きされます。

例

次に、HTTP に準拠していないトラフィックの転送を許可する例を示します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
hostname(config-http-map)#
```

関連コマンド

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

strip-group

このコマンドは、user@realm の形式で受信されるユーザ名にのみ適用されます。レルムは、「@」デリミタを使用してユーザ名に追加される管理ドメインです（juser@abc など）。

グループ除去処理をイネーブルまたはディセーブルにするには、トンネル グループ一般属性モードで **strip-group** コマンドを使用します。セキュリティ アプライアンスでは、VPN クライアントによって提示されるユーザ名からグループ名を取得して、IPSec 接続のトンネル グループを選択します。グループ除去処理をイネーブルにすると、セキュリティ アプライアンスでは、ユーザ名のユーザ部分のみを認可/認証のために送信します。それ以外の場合（ディセーブルの場合）、セキュリティ アプライアンスではレルムを含むユーザ名全体を送信します。

グループ除去処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

strip-group

no strip-group

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル タイプだけに適用できます。

（注） MSCHAPv2 の制限により、MSCHAPv2 を PPP 認証に使用すると、トンネル グループのスイッチングを実行できません。MSCHAPv2 中のハッシュ計算はユーザ名の文字列にバインドされます（ユーザ + 区切り + グループなど）。

例

次に、IPSec リモート アクセス タイプの「remotegrp」という名前のリモート アクセス トンネル グループを設定し、一般コンフィギュレーション モードを開始し、「remotegrp」という名前のトンネル グループをデフォルトのグループ ポリシーとして設定して、そのトンネル グループに対してグループ除去をイネーブルにする例を示します。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-group
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

strip-realm

レルム除去処理をイネーブルまたはディセーブルにするには、トンネル グループ一般属性コンフィギュレーション モードで **strip-realm** コマンドを使用します。レルム除去処理によって、ユーザ名を認証サーバまたは認可サーバに送信するときに、ユーザ名からレルムが削除されます。レルムは、@ デリミタを使用してユーザ名に追加される管理ドメインです（username@realm など）。このコマンドをイネーブルにすると、セキュリティ アプライアンスでは、ユーザ名のユーザ部分のみを認可/認証のために送信します。それ以外の場合、セキュリティ アプライアンスではユーザ名全体を送信します。

レルム除去処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

strip-realm

no strip-realm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル タイプだけに適用できます。

例

次に、IPSec リモート アクセス タイプの「remotegrp」という名前のリモート アクセス トンネル グループを設定し、一般コンフィギュレーション モードを開始し、「remotegrp」という名前のトンネル グループをデフォルトのグループ ポリシーとして設定して、そのトンネル グループに対してレルム除去をイネーブルにする例を示します。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-realm
```

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 グループまたは指定されたトンネル グループをクリアします。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

storage-key

セッション間に保管されるデータを保護するストレージ キーを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **storage-key** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

storage- key { **none** | **value** <*string*>}

no storage-key

構文の説明

string	ストレージ キーの値として使用するストリングを指定します。この文字列は最大 64 文字まで使用できます。

デフォルト

デフォルトは **none** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ストレージ キーの値にはスペース以外の任意の文字を使用できますが、標準的な英数字セット（0 ～ 9 および a ～ z）のみを使用することを推奨します。

例

次に、ストレージ キーを値 abc123 に設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# storage-key value abc123
```

関連コマンド

コマンド	説明
storage-objects	セッションとセッションの間に保存されたデータのストレージ オブジェクトを設定します。

storage-objects

セッション間に保管されるデータについて使用するストレージ オブジェクトを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **storage-objects** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

storage- objects { **none** | **value** <*string*>}

no storage-objects

構文の説明

string	ストレージ オブジェクトの名前を指定します。この文字列は最大 64 文字まで使用できます。

デフォルト

デフォルトは **none** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ストレージ オブジェクト名にはスペースおよびカンマ以外の任意の文字を使用できますが、標準的な英数字セット（0 ～ 9 および a ～ z）のみを使用することを推奨します。ストリング内でストレージ オブジェクトの名前を区切るには、カンマをスペースなしで使用します。

例

次に、ストレージ オブジェクト名を cookies および xyz456 に設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# storage-object value cookies,xyz456
```

関連コマンド

コマンド	説明
storage-key	セッション間に保管されるデータに対して使用するストレージ キーを設定します。
user-storage	セッション間にユーザ データを保管するための場所を設定します。

subject-name（クリプト CA 証明書マップ）

IPSec ピア証明書のサブジェクト DN にルール エントリが適用されることを指定するには、クリプト CA 証明書マップ コンフィギュレーション モードで **subject-name** コマンドを使用します。サブジェクト名を削除するには、このコマンドの **no** 形式を使用します。

subject-name [**attr** *tag*] **eq | ne |co | nc** *string*]

no subject-name [**attr** *tag*] **eq | ne |co | nc** *string*]

構文の説明

attr *tag*	証明書 DN の指定された属性値のみがルール エントリ ストリングと比較されることを指定します。タグ値は次のとおりです。 DNQ = DN 修飾子 GENQ = 世代識別子 I = イニシャル GN = 姓名の名 N = 名前 SN = 姓名の姓 IP = IP アドレス SER = シリアル番号 UNAME = 非構造化名 EA = 電子メール アドレス T = タイトル O = 組織名 L = 地名 SP = 州 / 都道府県 C = 国 OU = 組織ユニット CN = 一般名
co	ルール エントリ ストリングが DN ストリングまたは指定された属性のサブストリングである必要があることを指定します。
eq	DN ストリングまたは指定された属性がルール ストリング全体と一致する必要があることを指定します。
nc	ルール エントリ ストリングが DN ストリングまたは指定された属性のサブストリングでないことが必要であることを指定します。
ne	DN ストリングまたは指定された属性がルール ストリング全体と一致しないことが必要であることを指定します。
string	照合される値を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	透過	シングル	コンテキスト	システム
クリプト CA 証明書マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、証明書マップ 1 に対して CA 証明書マップ モードを開始し、証明書サブジェクト名の組織属性が Central と等しくなる必要があることを指定するルール エントリを作成する例を示します。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr o eq central
hostname(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
issuer-name	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

subject-name（クリプト CA トラスト ポイント）

指定したサブジェクト DN を登録時に証明書に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **subject-name** コマンドを使用します。これは、証明書を使用する人またはシステムです。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

subject-name *X.500_name*

no subject-name

構文の説明

X.500_name	X.500 認定者名を定義します。属性と値のペアを区切るには、カンマを使用します。カンマやスペースを含む値は、引用符で囲みます。たとえば、**cn=crl,ou=certs,o="cisco systems, inc.",c=US** です。最大長は 500 文字です。

デフォルト

デフォルト設定では、サブジェクト名は含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始し、URL https//:frog.phoobin.com での自動登録を設定し、サブジェクト DN OU certs をトラストポイント central の登録要求に含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://frog.phoobin.com/
hostname(ca-trustpoint)# subject-name ou=certs
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment url	CA に対する登録用の URL を指定します。

subject-name-default

ローカル CA サーバが発行するすべてのユーザ証明書でユーザ名に追加される一般的なサブジェクト名 DN を指定するには、CA サーバ コンフィギュレーション モードで **subject-name-default** コマンドを使用します。サブジェクト名 DN をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

subject-name-default *dn*

no subject-name-default

構文の説明

dn	ローカル CA サーバが発行するすべてのユーザ証明書でユーザ名に含める一般的なサブジェクト名 DN を指定します。サポートされている DN 属性は、cn（一般名）、ou（組織ユニット）、ol（組織の地名）、st（州）、ea（電子メール アドレス）、c（会社）、t（タイトル）、および sn（姓名の姓）です。属性と値のペアを区切るには、カンマを使用します。カンマやスペースを含む値は、引用符で囲みます。*dn* に使用できる文字数は最大 500 文字です。

デフォルト

このコマンドは、デフォルトのコンフィギュレーションの一部ではありません。このコマンドでは、証明書のデフォルトの DN を指定します。ユーザ入力に DN がある場合、このコマンドはセキュリティ アプライアンスによって無視されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

subject-name-default コマンドでは、発行される証明書のサブジェクト名を構成するユーザ名で使用される、共通の一般的な認定者名を指定します。この目的には、*dn* 値は cn=username で十分です。このコマンドによって、ユーザごとに個別にサブジェクト名 DN を定義する必要がなくなります。

セキュリティ アプライアンスでは、このコマンドは、ユーザ入力で DN が指定されない場合に、証明書を発行するときにのみ使用されます。**crypto ca server user-db add** dn *dn* コマンドを使用してユーザが追加される場合、DN フィールドは任意です。

例

次に、DN を指定する例を示します。

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma,
c="cisco systems, inc."
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。
lifetime	CA 証明書、発行済みの証明書、または CRL のライフタイムを指定します。

summary-address（OSPF）

OSPF の集約アドレスを作成するには、ルータ コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスまたは特定のサマリー アドレス オプションを削除するには、このコマンドの **no** 形式を使用します。

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

構文の説明

addr	アドレス範囲に対して指定されるサマリー アドレスの値。
mask	集約ルートに対して使用される IP サブネット マスク。
not-advertise	（任意）指定されたプレフィックス/マスク ペアと一致するルートを抑制します。
tag *tag_value*	（任意）各外部ルートに付けられた 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効値の範囲は、0 ～ 4294967295 です。

デフォルト

デフォルトの設定は次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックス/マスク ペアと一致するルートは抑制されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

他のルーティング プロトコルから学習したルートをサマライズできます。このコマンドを OSPF に対して使用すると、OSPF Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）により、このアドレスの対象となる再配布されるすべてのルートの集約として、1 つの外部ルートがアドバタイズされます。このコマンドでは、OSPF に再配布されている、他のルーティング プロトコルからのルートのみが集約されます。OSPF エリア間のルート集約には **area range** コマンドを使用します。

summary-address コマンドをコンフィギュレーションから削除するには、このコマンドの no 形式を、任意のキーワードまたは引数を指定しないで使用します。コンフィギュレーションの summary コマンドからオプションを削除するには、このコマンドの **no** 形式を使用して、削除するオプションを指定します。詳細については、「例」を参照してください。

例

次の例では、**tag** を 3 に設定してルート集約を設定しています。

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次の例に、**no** 形式の **summary-address** コマンドをオプションとともに使用して、オプションをデフォルト値に戻す方法を示します。この例では、先の例で 3 に設定された **tag** 値が、**summary-address** コマンドから削除されます。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次の例では、コンフィギュレーションから **summary-address** コマンドを削除しています。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
area range	エリア境界でルートを統合および集約します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf summary-address	各 OSPF ルーティング プロセスのサマリー アドレス設定を表示します。

summary-address（EIGRP）

特定のインターフェイスの EIGRP のサマリーを設定するには、インターフェイス コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスを削除するには、このコマンドの **no** 形式を使用します。

summary-address *as-number addr mask* [*admin-distance*]

no summary-address *as-number addr mask*

構文の説明

as-number	自律システム番号。これは、EIGRP ルーティング プロセスの自律システム番号と同じである必要があります。
addr	サマリー IP アドレス。
mask	IP アドレスに適用されるサブネット マスク。
admin-distance	（任意）集約ルートのアドミニストレーティブ ディスタンス。有効な値は、0 ～ 255 です。指定されていない場合、デフォルト値は 5 です。

デフォルト

デフォルトの設定は次のとおりです。

- EIGRP は、単一のホスト ルートの場合でも、ルートをネットワーク レベルに自動的に集約します。
- EIGRP 集約ルートのアドミニストレーティブ ディスタンスは 5 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、EIGRP はサブネット ルートをネットワーク レベルに集約します。自動ルート集約をディセーブルにするには、**no auto-summary** コマンドを使用します。**summary-address** コマンドを使用すると、サブネット ルート集約をインターフェイス単位で手動で定義できます。

例

次の例では、**tag** を 3 に設定してルート集約を設定しています。

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

次の例に、**no** 形式の **summary-address** コマンドをオプションとともに使用して、オプションをデフォルト値に戻す方法を示します。この例では、先の例で 3 に設定された **tag** 値が、**summary-address** コマンドから削除されます。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

次の例では、コンフィギュレーションから **summary-address** コマンドを削除しています。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
auto-summary	EIGRP ルーティング プロセスのサマリー アドレスを自動的に作成します。

sunrpc-server

SunRPC サービス テーブルのエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。SunRPC サービス テーブルのエントリをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [**-** *port*] **timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [*- port]* **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

構文の説明

ifc_name	サーバ インターフェイス名。
ip_addr	SunRPC サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* [**-** *port*]	SunRPC プロトコルのポート範囲を指定します。
port- *port*	（任意）SunRPC プロトコルのポート範囲を指定します。
protocol tcp	SunRPC トランスポート プロトコルを指定します。
protocol udp	SunRPC トランスポート プロトコルを指定します。
service	サービスを指定します。
service_type	**sunrpcinfo** コマンドで指定した SunRPC サービス プログラム番号を設定します。
timeout *hh:mm:ss*	SunRPC サービス トラフィックへのアクセスが終了するまでのタイムアウト アイドル時間を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SunRPC サービス テーブルは、timeout で指定された時間、確立された SunRPC セッションに基づいて、SunRPC トラフィックがセキュリティ アプライアンスを通過するのを許可するために使用します。

例

次に、SunRPC サービス テーブルを作成する例を示します。

```
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスからの Sun リモート プロセッサ コール サービスをクリアします。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

support-user-cert-validation

現在のトラストポイントが、リモート ユーザ証明書を発行した CA に対して認証されている場合に、このトラストポイントに基づいてリモート証明書を検証するには、クリプト CA トラストポイント コンフィギュレーション モードで **support-user-cert-validation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

support-user-cert-validation

no support-user-cert-validation

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定では、ユーザ証明書の検証がサポートされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、同じ CA に対して 2 つのトラストポイントを保持できます。この場合は、同じ CA から 2 つの異なるアイデンティティ証明書が発行されます。トラストポイントが、この機能をイネーブルにしている別のトラストポイントにすでに関連付けられている CA に対して認証される場合、このオプションは自動的にディセーブルになります。これにより、パス検証パラメータの選択であいまいさが生じないようになります。ユーザが、この機能をイネーブルにした別のトラストポイントにすでに関連付けられている CA に認証されたトラストポイントでこの機能を有効化しようとした場合、アクションは許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central でユーザ検証を受け入れることができるようにする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# support-user-cert-validation
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。

svc ask

セキュリティ アプライアンスがリモート SSL VPN クライアント ユーザに対してクライアントのダウンロードを促せるようにするには、グループ ポリシー WebVPN またはユーザ名 webvpn コンフィギュレーション モードから **svc ask** 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、このコマンドの no 形式を使用します。

svc ask {**none** | **enable** [**default** {**webvpn** | **svc**} **timeout** *value*]}

no svc ask none [**default** {**webvpn** | **svc**}]

構文の説明

none	デフォルト アクションをただちに実行します。
enable	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動してユーザ応答を無期限に待機します。
default svc timeout *value*	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション（クライアントのダウンロード）を実行します。
default webvpn timeout *value*	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション（WebVPN ポータル ページの表示）を実行します。

デフォルト

このコマンドのデフォルトは、**svc ask none default webvpn** です。セキュリティ アプライアンスによって、クライアントレス接続のポータル ページがただちに表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

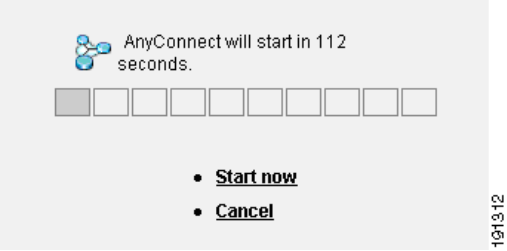
コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

図 31-1 に、**default svc timeout** *value* または **default webvpn timeout** *value* が設定された場合にリモート ユーザに表示されるプロンプトを示します。

図 31-1　SSL VPN Client のダウンロードに関してリモート ユーザに表示されるプロンプト



例

次に、セキュリティ アプライアンスを設定して、リモート ユーザにクライアントのダウンロードを要求するか、ポータル ページに移動して、ユーザの応答を 10 秒待機してからクライアントをダウンロードするように設定する例を示します。

```
hostname(config-group-webvpn)# svc ask enable default svc timeout 10
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

svc compression

特定のグループまたはユーザについて、SSL VPN 接続での http データの圧縮をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc compression** コマンドを使用します。

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

構文の説明

deflate	グループまたはユーザに対して圧縮をイネーブルにすることを指定します。
none	そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

デフォルト

デフォルトでは、圧縮は *none*（ディセーブル）に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

SSL VPN 接続の場合、webvpn コンフィギュレーション モードで設定された **compression** コマンドによって、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定された **svc compression** コマンドは上書きされます。

例

次の例では、グループ ポリシー sales に対して SVC 圧縮はディセーブルです。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
```

関連コマンド

コマンド	説明
compression	すべての SSL、WebVPN、および IPSec VPN 接続で、圧縮をイネーブルにします。
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。

svc dpd-interval

Dead Peer Detection（DPD; デッド ピア検出）をセキュリティ アプライアンスでイネーブルにし、リモート クライアントとセキュリティ アプライアンスのいずれかで SSL VPN 接続を介した DPD を実行する頻度を設定するには、グループ ポリシーまたはユーザ名 webvpn モードで **svc dpd-interval** コマンドを使用します。

svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

構文の説明

gateway *seconds*	セキュリティ アプライアンスで DPD が実行される頻度（30 ～ 3600 秒）を指定します。
gateway none	セキュリティ アプライアンスで実行される DPD をディセーブルにします。
client *seconds*	クライアントで DPD が実行される頻度（30 ～ 3600 秒）を指定します。
client none	クライアントで実行される DPD をディセーブルにします。

デフォルト

デフォルトでは、DPD はイネーブルであり、セキュリティ アプライアンス（ゲートウェイ）とクライアントの両方で 30 秒に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(3)	デフォルト設定が、ディセーブルから、セキュリティ アプライアンス（ゲートウェイ）とクライアントの両方で 30 秒に変更されました。

例

次の例では、ユーザは、既存のグループ ポリシー *sales* について、セキュリティ アプライアンス（ゲートウェイ）で実行される DPD の頻度を 3000 秒に設定し、クライアントで実行される DPD の頻度を 1000 秒に設定します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dpd-interval gateway 3000
hostname(config-group-webvpn)# svc dpd-interval client 1000
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc keepalive	リモート コンピュータ上のクライアントからセキュリティ アプライアンスにキープアライブ メッセージが SSL VPN 接続で送信される頻度を指定します。
svc keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
svc rekey	SSL VPN 接続でクライアントがキーの再生成を実行できるようにします。

svc dtls enable

Cisco AnyConnect VPN Client との SSL VPN 接続を確立している特定のグループまたはユーザのインターフェイスで Datagram Transport Layer Security（DTLS）接続をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで **dtls enable** コマンドを使用します。

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

dtls enable *interface*

no dtls enable *interface*

構文の説明

interface	インターフェイスの名前。

デフォルト

デフォルトではイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

DTLS をイネーブルにすると、SSL VPN 接続を確立している AnyConnect クライアントで、2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用できます。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

DTLS をイネーブルにしない場合、SSL VPN 接続を確立する AnyConnect クライアント ユーザは SSL トンネル経由でだけ接続できます。

このコマンドでは、特定のグループまたはユーザについて DTLS をイネーブルにします。すべての AnyConnect クライアント ユーザについて DTLS をイネーブルにするには、webvpn コンフィギュレーション モードで **dtls enable** コマンドを使用します。

例

次に、グループ ポリシー *sales* のグループ ポリシー webvpn コンフィギュレーション モードを開始し、DTLS をイネーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dtls enable
```

関連コマンド

コマンド	説明
dtls port	DTLS の UDP ポートを指定します。
svc dtls	SSL VPN 接続を確立するグループまたはユーザに対して、DTLS をイネーブルにします。
vpn-tunnel-protocol	セキュリティ アプライアンスがリモート アクセス用に許可する VPN プロトコル（SSL を含む）を指定します。

svc enable

セキュリティ アプライアンスがリモート コンピュータに SSL VPN クライアントをダウンロードできるようにするには、webvpn コンフィギュレーション モードで **svc enable** 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、このコマンドの **no** 形式を使用します。

svc enable

no svc enable

デフォルト

このコマンドのデフォルトはディセーブルです。セキュリティ アプライアンスによってクライアントはダウンロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

no svc enable コマンドを入力しても、アクティブなセッションは終了しません。

例

次の例では、ユーザはセキュリティ アプライアンスによってクライアントをダウンロードできるようにします。

```
(config)# webvpn
(config-webvpn)# svc enable
```

関連コマンド

コマンド	説明
show webvpn svc	セキュリティ アプライアンスにインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
svc localization	Cisco AnyConnect VPN Client にダウンロードされたローカリゼーション ファイルを保管するために使用するパッケージ ファイルを指定します。

svc profiles	セキュリティ アプライアンスによって Cisco AnyConnect VPN Client にダウンロードされるプロファイルを保管するために使用するファイルの名前を指定します。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開する SSL VPN クライアント パッケージ ファイルを指定します。

svc image

リモート PC へのダウンロード用にセキュリティ アプライアンスによってキャッシュ メモリに展開されている SSL VPN クライアント パッケージ ファイルを指定するには、webvpn コンフィギュレーション モードで **svc image** 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、このコマンドの **no** 形式を使用します。

svc image *filename order* [**regex** *expression*]

no svc image *filename order* [**regex** *expression*]

構文の説明

filename	パッケージ ファイルのファイル名を最大 255 文字で指定します。
order	クライアント パッケージ ファイルが複数である場合は、*order* によってパッケージ ファイルの順序（1 ～ 65535）を指定します。セキュリティ アプライアンスでは、オペレーティング システムと一致するまで、指定した順序に従って、各クライアントの一部をリモート PC にダウンロードします。
regex *expression*	ブラウザから渡される User-Agent ストリングと照合するためにセキュリティ アプライアンスによって使用されるストリングを指定します。

デフォルト

デフォルトの順序は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。
8.0(1)	**regex** *expression* 引数が追加されました。

使用上のガイドライン

パッケージ ファイルの番号付けにより、セキュリティ アプライアンスが、オペレーティング システムと一致するまで、パッケージ ファイルの一部をリモート PC にダウンロードする順序が確立されます。最も番号の小さいパッケージ ファイルが最初にダウンロードされます。したがって、リモート PC で最も一般的に使用されるオペレーティング システムと一致するパッケージ ファイルに、最も小さい番号を割り当てる必要があります。

デフォルトの順序は 1 です。*order* 引数を指定しない場合は、**svc image** コマンドを入力するたびに、以前に番号 1 と見なされたイメージに上書きします。

クライアント パッケージ ファイルごとに任意の順序で **svc image** コマンドを入力できます。たとえば、2 番め（*order* 2）にダウンロードされるパッケージ ファイルを指定してから、最初（*order* 1）にダウンロードされるパッケージ ファイルを指定する **svc image** コマンドを入力できます。

モバイル ユーザの場合、**regex** keyword を使用して、モバイル デバイスの接続時間を短縮できます。ブラウザがセキュリティ アプライアンスに接続するとき、User-Agent ストリングが HTTP ヘッダーに含められます。セキュリティ アプライアンスによってストリングが受信され、そのストリングがあるイメージ用に設定された式と一致すると、そのイメージがただちにダウンロードされます。この場合、他のクライアント イメージはテストされません。

セキュリティ アプライアンスでは、SSL VPN クライアントと Cisco Secure Desktop（CSD）の両方のパッケージ ファイルがキャッシュ メモリに展開されます。セキュリティ アプライアンスでパッケージ ファイルを正常に展開するには、パッケージ ファイルのイメージとファイルを保管するのに十分なキャッシュ メモリが必要です。

パッケージの展開に十分なキャッシュ メモリがないことをセキュリティ アプライアンスが検出した場合、コンソールにエラー メッセージが表示されます。次に、**svc image** コマンドを使用してパッケージ ファイルをインストールしようとした後でレポートされるエラー メッセージの例を示します。

```
hostname(config-webvpn)# svc image disk0:/vpn-win32-Release-2.0.0070-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

パッケージ ファイルをインストールしようとしたときにこのエラーが発生した場合は、グローバル コンフィギュレーション モードで **dir cache:/** コマンドを使用して、残っているキャッシュ メモリの量と以前にインストールしたパッケージのサイズを調べます。それに応じて、webvpn コンフィギュレーション モードで **cache-fs limit** コマンドを使用して、キャッシュ サイズの制限を調整します。

例

次の例では、**show webvpn svc** コマンドの出力により、windows.pkg ファイルの順序番号が 1 であり、windows2.pkg ファイルの順序番号が 15 であることが示されます。リモート コンピュータによって接続が確立されるときに、windows.pkg ファイルが最初にダウンロードされます。このファイルがオペレーティング システムと一致しない場合、windows2.pkg ファイルがダウンロードされます。

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows2.pkg 15
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

次に、ユーザは **svc image** コマンドを使用してパッケージ ファイルの順序を変更します。windows2.pkg ファイルをリモート PC にダウンロードされる最初のファイルとし、windows.pkg ファイルを 2 番めにダウンロードされるようにします。

```
hostname(config-webvpn)# svc image windows2.pkg 10
hostname(config-webvpn)# svc image windows.pkg 20
```

show webvpn svc コマンドを再入力すると、ファイルの新しい順序が表示されます。

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows2.pkg 10
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows.pkg 20
  CISCO STC win2k+ 1.0.0
  1,0,0,164
```

```
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

次に、CSD イメージ（sdesktop 内に存在）と SSL VPN クライアント イメージ（stc 内に存在）によって約 5.44 MB のキャッシュ メモリが使用されている例を示します。十分なキャッシュ メモリを作成するために、ユーザがキャッシュ サイズの制限を 6 MB に設定しています。

```
hostname(config-webvpn)# dir cache:

Directory of cache:/

0      drw-  0           17:06:55 Nov 13 2006  sdesktop
0      drw-  0           16:46:54 Nov 13 2006  stc

5435392 bytes total (4849664 bytes free)

hostname(config-webvpn)# cache-fs limit 6
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
cache-fs limit	キャッシュ メモリのサイズを制限します。
dir cache:	キャッシュ メモリの内容を表示します。
show webvpn svc	セキュリティ アプライアンスにインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
svc enable	セキュリティ アプライアンスによってクライアントをリモート コンピュータにダウンロードできるようにします。

svc keepalive

SSL VPN 接続でリモート クライアントからセキュリティ アプライアンスに送信されるキープアライブ メッセージの頻度を設定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc keepalive** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

svc keepalive {**none** | *seconds*}

no svc keepalive {**none** | *seconds*}

構文の説明

none	キープアライブ メッセージをディセーブルにします。
seconds	キープアライブ メッセージをイネーブルにし、メッセージの頻度（15 ～ 600 秒）を指定します。

デフォルト

デフォルトは 20 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(3)	デフォルト設定がディセーブルから 20 秒に変更されました。

使用上のガイドライン

従来の Cisco SSL VPN Client（SVC）と Cisco AnyConnect VPN Client の両方で、セキュリティ アプライアンスへの SSL VPN 接続を確立するときにキープアライブ メッセージを送信できます。

接続をアイドル状態で維持できる時間がデバイスによって制限されている場合も、プロキシ、ファイアウォール、または NAT デバイスを経由した SSL VPN 接続が確実に開いたままで保たれるように、キープアライブ メッセージの頻度を調整できます（*seconds* で指定）。

また、頻度を調整すると、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース アプリケーションをアクティブに実行していない場合でも、クライアントは切断および再接続されません。

（注）　キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルにすると、フェールオーバー イベントの際に、SSL VPN クライアント セッションはスタンバイ デバイスに引き継がれません。

例

次の例では、ユーザは、*sales* という名前の既存のグループ ポリシーについて、セキュリティ アプライアンスを設定し、クライアントがキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるようにします。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに SSL VPN クライアントをイネーブルにします。または、要求します。
svc dpd-interval	セキュリティ アプライアンスで Dead Peer Detection（DPD; デッド ピア検出）をイネーブルにし、クライアントまたはセキュリティ アプライアンスによって DPD が実行される頻度を設定します。
svc keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
svc rekey	セッションでクライアントがキーの再生成を実行できるようにします。

svc keep-installer

リモート PC への SSL VPN クライアントの永続インストールをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc keep-installer** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

svc keep-installer {**installed** | **none**}

no svc keep-installer {**installed** | **none**}

構文の説明

installed	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続に備えてリモート PC にインストールされたままとなります。
none	アクティブな接続の終了後にクライアントがリモート コンピュータからアンインストールされることを指定します。

デフォルト

デフォルトでは、クライアントの永続インストールがイネーブルです。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次の例では、ユーザはグループ ポリシー webvpn コンフィギュレーション モードを開始し、セッションの終了時にクライアントを削除するようにグループ ポリシーを設定します。

```
hostname(config-group-policy)#webvpn
hostname(config-group-webvpn)# svc keep-installer none
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn svc	セキュリティ アプライアンスにインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
svc	特定のグループまたはユーザに対してクライアントをイネーブルまたは必須にします。
svc enable	セキュリティ アプライアンスがクライアント ファイルをリモート PC にダウンロードできるようにします。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

svc modules

オプション機能のために AnyConnect SSL VPN Client で必要となるオプション モジュールの名前を指定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc modules** 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、このコマンドの **no** 形式を使用します。

svc modules {**none** | **value** *string*}

no svc modules {**none** | **value** *string*}

構文の説明

string	オプション モジュールの名前（最大 256 文字）。複数のストリングを指定する場合は、カンマで区切ります。

デフォルト

デフォルトは none です。セキュリティ アプライアンスによってオプション モジュールはダウンロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ダウンロード時間を最小にするために、クライアントでは、サポートする各機能に必要なモジュールのダウンロード（セキュリティ アプライアンスから）のみを要求します。**svc modules** コマンドにより、セキュリティ アプライアンスでこれらのモジュールをダウンロードできます。**none** を選択すると、セキュリティ アプライアンスによって基本的なファイルがダウンロードされ、オプションのモジュールはダウンロードされません。

vpngina ストリングを使用して、Start Before Logon（SBL）機能をイネーブルにします。このストリングにより、セキュリティ アプライアンスでは AnyConnect クライアント VPN 接続用の Graphical Identification and Authentication（GINA）をダウンロードできます。

すべてのクライアント機能に入力する値の一覧については、Cisco AnyConnect VPN Client のリリースノートを参照してください。

例

次の例では、ユーザはグループ ポリシー *telecommuters* でグループ ポリシー属性モードを開始し、そのグループ ポリシーで webvpn コンフィギュレーション モードを開始し、ストリング *vpngina* を指定します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

関連コマンド

コマンド	説明
show webvpn svc	セキュリティ アプライアンスのキャッシュ メモリにロードされていてダウンロード可能な SSL VPN クライアントについての情報を表示します。
svc enable	特定のグループまたはユーザに対して、SSL VPN クライアントをイネーブルにします。
svc image	リモート PC へのダウンロード用にセキュリティ アプライアンスによってキャッシュ メモリに展開されている SSL VPN クライアント パッケージ ファイルを指定します。

svc mtu

Cisco AnyConnect VPN Client によって確立された SSL VPN 接続の MTU サイズを調整するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc mtu** 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、このコマンドの **no** 形式を使用します。

svc mtu *size*

no svc mtu *size*

構文の説明

size	MTU サイズ（バイト単位）。256 ～ 1406 バイトです。

デフォルト

デフォルトのサイズは 1406 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、AnyConnect クライアントのみに影響します。Cisco SSL VPN Client（SVC）は、異なる MTU サイズに調整できません。

デフォルトのグループ ポリシーでのこのコマンドのデフォルトは、**no svc mtu** です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

このコマンドは、SSL のみで確立された AnyConnect クライアント接続と、DTLS を使用する SSL で確立された AnyConnect クライアント接続に影響します。

例

次に、グループ ポリシー *telecommuters* について、MTU サイズを 500 バイトに設定する例を示します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc mtu 500
```

関連コマンド

コマンド	説明
svc keep-installer	クライアントの自動アンインストール機能をディセーブルにします。初期ダウンロード後、接続が終了した後もクライアントはリモート PC 上に残ります。
svc dtls	SSL VPN 接続を確立するクライアントに対して DTLS をイネーブルにします。
show run webvpn	**svc** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。

svc profiles（グループ ポリシーまたはユーザ名属性）

Cisco AnyConnect VPN Client ユーザにダウンロードされるプロファイル パッケージを指定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで、**svc profile** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

svc profiles {**value** *profile* | **none**}

no svc profiles {**value** *profile* | **none**}

構文の説明

profile	プロファイル名。

デフォルト

デフォルトは none です。セキュリティ アプライアンスによってプロファイルはダウンロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドをグループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで入力すると、セキュリティ アプライアンスによってグループ ポリシーまたはユーザ名に基づいてプロファイルをユーザにダウンロードできます。プロファイルをすべてのユーザにダウンロードするには、このコマンドを webvpn コンフィギュレーション モードで使用します。

プロファイルは設定パラメータのグループであり、クライアントによって、ホスト コンピュータの名前やアドレスを含めて、クライアント ユーザ インターフェイスに表示される接続エントリの設定に使用されます。AnyConnect ユーザ インターフェイスを使用して、プロファイルを作成および保存できます。また、テキスト エディタでこのファイルを編集し、ユーザ インターフェイスからは設定できないパラメータの詳細を設定することもできます。

クライアント インストールには、編集可能なプロファイル テンプレート（AnyConnectProfile.tmpl）が含まれており、別のプロファイル ファイルを作成するための基本として使用できます。プロファイルの編集について詳しくは、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

例

次の例では、ユーザは使用可能なプロファイルを表示する **svc profiles value** コマンドを照会します。

```
asa1(config-group-webvpn)# svc profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

ユーザはその後、プロファイル *sales* を使用するようグループ ポリシーを設定しています。

```
asa1(config-group-webvpn)# svc profiles sales
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザに SSL VPN クライアントをイネーブルにします。または、要求します。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

svc profiles（webvpn）

セキュリティ アプライアンスによってキャッシュ メモリにロードされて、Cisco AnyConnect VPN Client ユーザのグループ ポリシーおよびユーザ属性で使用可能となるプロファイル パッケージとして、ファイルを指定するには、webvpn コンフィギュレーション モードで **svc profile** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除し、セキュリティ アプライアンスによってパッケージ ファイルがキャッシュ メモリからアンロードされるようにするには、このコマンドの **no** 形式を使用します。

svc profiles {*profile path*}

no svc profiles {*profile path*}

構文の説明

path	セキュリティ アプライアンスのフラッシュ メモリ内のプロファイル ファイルのパスおよびファイル名。
profile	キャッシュ内に作成するプロファイルの名前。

デフォルト

デフォルトは none です。プロファイル パッケージはセキュリティ アプライアンスによってキャッシュ メモリにロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

プロファイルは設定パラメータのグループであり、AnyConnect クライアントによって、ホスト コンピュータの名前やアドレスを含めて、ユーザ インターフェイスに表示される接続エントリの設定に使用されます。クライアント ユーザ インターフェイスを使用して、プロファイルを作成および保存できます。

また、テキスト エディタでこのファイルを編集し、ユーザ インターフェイスからは設定できないパラメータの詳細を設定することもできます。クライアント インストールには、編集可能なプロファイル テンプレート（AnyConnectProfile.tmpl）が含まれており、別のプロファイル ファイルを作成するための基本として使用できます。プロファイルの編集について詳しくは、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

新しいプロファイルを作成してフラッシュ メモリにアップロードした後、webvpn コンフィギュレーション モードで **svc profiles** コマンドを使用して、セキュリティ アプライアンスに対して XML ファイルをプロファイルとして指定します。このコマンドによって、ファイルはセキュリティ アプライアン

ス上のキャッシュ メモリにロードされます。次に、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **svc profiles** コマンドを使用して、グループまたはユーザのプロファイルを指定できます。

例

次の例では、ユーザはまずクライアントのインストールに付属する AnyConnectProfile.tmpl ファイルから 2 つの新規プロファイル ファイル（sales_hosts.xml と engineering_hosts.xml）を作成し、セキュリティ アプライアンスのフラッシュ メモリにアップロードしています。

さらに、ユーザはそれらのファイルを AnyConnect のプロファイルとしてセキュリティ アプライアンスに指定し、*sales* と *engineering* という名前を指定しています。

```
asa1(config-webvpn)# svc profiles sales disk0:sales_hosts.xml
asa1(config-webvpn)# svc profiles engineering disk0:engineering_hosts.xml
```

dir cache:stc/profiles コマンドを入力すると、キャッシュ メモリにロードされたプロファイルが表示されます。

```
asa1(config-webvpn)# dir cache:stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg

2428928 bytes total (18219008 bytes free)
asa1(config-webvpn)#
```

これで、これらをグループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードでの **svc profiles** コマンドで使用できます。

```
asa1(config)# group-policy sales attributes
asa1(config-group-policy)# webvpn
asa1(config-group-webvpn)# svc profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc image	リモート PC へのダウンロード用にセキュリティ アプライアンスによってキャッシュ メモリに展開されている SSL VPN パッケージ ファイルを指定します。

svc rekey

SSL VPN 接続でリモート クライアントがキーの再生成を実行できるようにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **svc rekey** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

構文の説明

method ssl	キーの再生成中に SSL の再ネゴシエーションが行われることを指定します。
method new-tunnel	キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
time *minutes*	セッションの開始からキーの再生成が発生するまでの時間（分）を指定します。4 ～ 10080（1 週間）の範囲です。
method none	キーの再生成をディセーブルにします。

デフォルト

デフォルトは none（ディセーブル）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

従来の Cisco SSL VPN Client（SVC）と Cisco AnyConnect VPN クライアントは、両方ともセキュリティ アプライアンスへの SSL VPN 接続上でキーの再作成を実行できます。

キーの再生成方法として SSL を設定することを推奨します。

例

次の例では、ユーザは、グループ ポリシー *sales* に属するリモート クライアントがキーの再生成時に SSL と再ネゴシエートし、セッションの開始後 30 分でキーの再生成が発生することを指定します。

```
hostname(config)# group-policy sales attributes
```

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc rekey method ssl
hostname(config-group-webvpn)# svc rekey time 30
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに対して AnyConnect クライアントをイネーブルまたは必須にします。
svc dpd-interval	Dead Peer Detection（DPD; デッド ピア検出）をセキュリティ アプライアンスでイネーブルにし、AnyConnect クライアントまたはセキュリティ アプライアンスのいずれかで DPD を実行する頻度を設定します。
svc keepalive	リモート コンピュータ上の AnyConnect クライアントからセキュリティ アプライアンスにキープアライブ メッセージが送信される頻度を指定します。
svc keep-installer	リモート コンピュータへの AnyConnect クライアントの永続インストールをイネーブルにします。

switchport access vlan

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport access vlan** コマンドを使用して、スイッチ ポートを VLAN に割り当てます。

switchport access vlan *number*

no switchport access vlan *number*

構文の説明

vlan *number*	このスイッチ ポートを割り当てる VLAN ID を指定します。VLAN ID の範囲は 1 ～ 4090 です。

デフォルト

デフォルトでは、すべてのスイッチ ポートが VLAN 1 に割り当てられています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

トランスペアレント ファイアウォール モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスで 2 つのアクティブ VLAN、Security Plus ライセンスで 3 つのアクティブ VLAN を設定でき、そのうちの 1 つはフェールオーバー用である必要があります。

ルーテッド モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスで最大 3 つのアクティブ VLAN、Security Plus ライセンスで最大 20 のアクティブ VLAN を設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。

switchport access vlan コマンドを使用して、1 つ以上の物理インターフェイスを各 VLAN に割り当てることができます。デフォルトでは、インターフェイスの VLAN モードはアクセス ポートになります（インターフェイスに関連付けられた 1 つの VLAN）。インターフェイスで複数の VLAN を渡すトランク ポートを作成する場合は、**switchport mode access trunk** コマンドを使用してモードをトランク モードに変更してから、**switchport trunk allowed vlan** コマンドを使用します。

例

次に、5 つの物理インターフェイスを 3 つの VLAN インターフェイスに割り当てる例を示します。

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport mode

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport mode** コマンドを使用して、VLAN モードをアクセス（デフォルト）またはトランクに設定します。

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

構文の説明

access	スイッチ ポートをアクセス モードに設定します。このモードでは、スイッチ ポートで 1 つの VLAN のみのトラフィックを渡すことができます。パケットは、802.1Q VLAN タグなしでスイッチ ポートから出ます。パケットがタグ付きでスイッチ ポートに入ると、パケットはドロップされます。
trunk	スイッチ ポートをトランク モードに設定します。そのため、複数の VLAN のトラフィックを渡すことができます。パケットは、802.1Q VLAN タグ付きでスイッチ ポートから出ます。パケットがタグなしでスイッチ ポートに入ると、パケットはドロップされます。

デフォルト

デフォルトでは、モードはアクセスです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
7.2(2)	1 つのトランクに制限されず、複数のトランク ポートを設定できるようになりました。

使用上のガイドライン

デフォルトでは、スイッチ ポートの VLAN モードはアクセス ポートになります（スイッチ ポートに関連付けられた 1 つの VLAN）。アクセス モードでは、**switchport access vlan** コマンドを使用してスイッチ ポートを VLAN に割り当てます。スイッチ ポートで複数の VLAN を渡すトランク ポートを作成する場合は、モードをトランク モードに設定してから、**switchport trunk allowed vlan** コマンドを使用して複数の VLAN をトランクに割り当てます。モードをトランク モードに設定し、**switchport trunk allowed vlan** コマンドを設定していない状態では、スイッチ ポートは「回線プロトコル ダウン」状態になり、トラフィック転送に参加できません。トランク モードが使用できるのは Security Plus ライセンスだけです。

モードをアクセス モードに設定しない限り、**switchport vlan access** コマンドは有効になりません。モードをトランク モードに設定しない限り、**switchport trunk allowed vlan** コマンドは有効になりません。

例

次に、VLAN 100 に割り当てられたアクセス モードのスイッチ ポートおよび VLAN 200 および 300 に割り当てられたトランク モードのスイッチ ポートを設定する例を示します。

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200,300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport monitor

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport monitor** コマンドを使用して、SPAN（スイッチ ポート モニタリングとも呼ばれる）をイネーブルにします。このコマンドを入力する対象のポート（宛先ポートと呼ばれる）では、指定した送信元ポートで送受信されるすべてのパケットのコピーを受信します。SPAN 機能を使用すると、トラフィックをモニタできるように、スニファを宛先ポートに接続できます。このコマンドを複数回入力して、複数の送信元ポートを指定できます。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。送信元ポートのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport monitor *source_port* [**tx** | **rx** | **both**]

no switchport monitor *source_port* [**tx** | **rx** | **both**]

構文の説明

source_port	モニタするポートを指定します。任意のイーサネット ポートおよび VLAN インターフェイス間でトラフィックを渡す Internal-Data0/1 バックプレーン ポートを指定できます。Internal-Data0/1 ポートはギガビット イーサネット ポートであるため、ファスト イーサネット宛先ポートをトラフィックによって過負荷にする場合があります。Internal-Data0/1 ポートは注意してモニタしてください。
tx	（任意）送信トラフィックのみをモニタすることを指定します。
rx	（任意）受信トラフィックのみをモニタすることを指定します。
both	（任意）送信トラフィックと受信トラフィックの両方をモニタすることを指定します。**both** がデフォルトです。

デフォルト

モニタするトラフィックのデフォルトのタイプは **both** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

SPAN をイネーブルにしない場合、スニファをスイッチ ポートの 1 つに接続すると、そのポートで送受信されるトラフィックのみがキャプチャされます。複数のポートで送受信されるトラフィックをキャプチャするには、SPAN をイネーブルにし、モニタするポートを指定する必要があります。

ネットワーク ループになる可能性があるため、SPAN 宛先ポートを別のスイッチに接続するときは注意してください。

例

次に、イーサネット 0/0 ポートとイーサネット 0/2 ポートをモニタする宛先ポートとして、イーサネット 0/1 ポートを設定する例を示します。

```
hostname(config)# interface ethernet 0/1
hostname(config-if)# switchport monitor ethernet 0/0
hostname(config-if)# switchport monitor ethernet 0/2
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。

switchport protected

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport protected** コマンドを使用して、スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信しないようにします。この機能により、あるスイッチ ポートが侵害された場合に、VLAN 上の他のスイッチ ポートに対して強固なセキュリティを提供します。

switchport protected

no switchport protected

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、インターフェイスは保護されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに **switchport protected** コマンドを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

保護されていないポートとの通信は、このコマンドによって制限されません。

例

次に、7 つのスイッチ ポートを設定する例を示します。イーサネット 0/4、0/5、および 0/6 は DMZ ネットワークに割り当てられ、相互から保護されます。

```
hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/5
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/6
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport trunk

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport trunk** コマンドを使用して、VLAN をトランク ポートに割り当てます。VLAN をトランクから削除するには、このコマンドの **no** 形式を使用します。

switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

no switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

構文の説明

allowed vlans *vlan_range*	トランク ポートに割り当てることができる 1 つ以上の VLAN を指定します。VLAN ID の範囲は 1 ～ 4090 です。 *vlan_range* は、次のいずれかの方法で指定できます。 • 単一の番号（n） • 範囲（n-x） 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。 5,7-10,13,45-100 カンマの代わりにスペースを入力できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。 このコマンドにネイティブ VLAN を含めることができますが、必須ではありません。ネイティブ VLAN は、このコマンドに含まれているかどうかに関係なく渡されます。
native vlan *vlan*	ネイティブ VLAN をトランクに割り当てます。ネイティブ VLAN 上のパケットは、トランク経由で送信されるときに変更されません。 たとえば、ポートに VLAN 2、3、および 4 が割り当てられており、VLAN 2 がネイティブ VLAN である場合、ポートを出る VLAN 2 上のパケットは 802.1Q ヘッダーによって変更されません。このポートに入るフレームで 802.1Q ヘッダーがないものは、VLAN 2 に渡されます。 各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

デフォルト

デフォルトでは、VLAN はトランクに割り当てられていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
7.2(2)	このコマンドは、スイッチ ポートごとに 4 つ以上の VLAN を許可するように変更されました。また、1 つのみに制限されず、複数のトランク ポートを設定できるようになりました。このコマンドで、VLAN ID を区切るためにスペースではなくカンマも使用されます。
7.2(4)/8.0(4)	**native vlan** キーワードを使用するネイティブ VLAN サポートが追加されました。

使用上のガイドライン

スイッチ ポートで複数の VLAN を渡すトランク ポートを作成する場合は、**switchport mode trunk** コマンドを使用してモードをトランク モードに設定してから、**switchport trunk** コマンドを使用して VLAN をトランクに割り当てます。このスイッチ ポートに少なくとも 1 つの VLAN を割り当てるまで、このスイッチ ポートでトラフィックを渡すことはできません。モードをトランク モードに設定し、**switchport trunk allowed vlan** コマンドを設定していない状態では、スイッチ ポートは「回線プロトコル ダウン」状態になり、トラフィック転送に参加できません。トランク モードが使用できるのは Security Plus ライセンスだけです。**switchport mode trunk** コマンドを使用してモードをトランク モードに設定しない限り、**switchport trunk** コマンドは有効になりません。

（注） このコマンドにはバージョン 7.2(1) との下位互換性はありません。VLAN を区切るカンマは 7.2(1) では認識されません。ダウングレードする場合は、VLAN をスペースで区切り、3 つの VLAN という制限を超えないようにしてください。

例

次に、7 つの VLAN インターフェイスを設定する例を示します。**failover lan** コマンドを使用して設定するフェールオーバー インターフェイスが含まれています。VLAN 200、201、および 202 は、イーサネット 0/1 でトランキングされています。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 201
hostname(config-if)# nameif dept1
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 202
hostname(config-if)# nameif dept2
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.3.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# switchport trunk native vlan 5
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。

synack-data

データが含まれる TCP SYNACK パケットのアクションを設定するには、tcp マップ コンフィギュレーション モードで **synack-data** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

synack-data {**allow** | **drop**}

no synack-data

構文の説明

allow	データが含まれる TCP SYNACK パケットを許可します。
drop	データが含まれる TCP SYNACK パケットをドロップします。

デフォルト

デフォルト アクションでは、データが含まれる TCP SYNACK パケットをドロップします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

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

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **synack-data**：tcp マップ コンフィギュレーション モードでは、**synack-data** などの数多くのコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、データが含まれる TCP SYNACK パケットを許可するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# tcp-map tmap
```

```
hostname(config-tcp-map)# synack-data allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

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

syn-data

データが含まれる SYN パケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

構文の説明

allow	データが含まれる SYN パケットを許可します。
drop	データが含まれる SYN パケットをドロップします。

デフォルト

デフォルトでは、SYN データが含まれるパケットは許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用して、SYN パケット内にデータが含まれるパケットをドロップします。

TCP の仕様によると、TCP 実装は SYN パケット内に含まれているデータを受け入れる必要があります。これは微妙であいまいな点であるため、一部の実装ではこのことが正しく処理されない場合があります。不適切なエンドシステム実装などの挿入攻撃に対する脆弱性を回避するために、SYN パケット内にデータが含まれるパケットをドロップすることを選択できます。

例

次に、データが含まれる SYN パケットをすべての TCP フローでドロップする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# syn-data drop
```

```
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

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

sysopt connection permit-vpn

VPN トンネルを介してセキュリティ アプライアンスに入り復号化されるトラフィックに対して、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用して、トラフィックがインターフェイス アクセス リストをバイパスできるようにします。グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection permit-vpn

no sysopt connection permit-vpn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、デフォルトでイネーブルになりました。また、インターフェイス アクセス リストのみがバイパスされます。グループ ポリシーまたはユーザ単位のアクセス リストは有効なままです。
7.1(1)	このコマンドは、**sysopt connection permit-ipsec** から変更されました。

使用上のガイドライン

デフォルトでは、セキュリティ アプライアンスによって、VPN トラフィックがセキュリティ アプライアンスのインターフェイスで終端することが許可されています。IKE または ESP（またはその他のタイプの VPN パケット）をインターフェイス アクセス リストで許可する必要はありません。デフォルトでは、復号化された VPN パケットのローカル IP アドレスのインターフェイス アクセス リストも必要ありません。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、コンフィギュレーションが簡略化され、セキュリティ アプライアンスのパフォーマンスはセキュリティ リスクを負うことなく最大化されます （グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます）。

no sysopt connection permit-vpn コマンドを入力して、インターフェイス アクセス リストをローカル IP アドレスに適用できます。アクセス リストを作成してインターフェイスに適用するには、**access-list** コマンドおよび **access-group** コマンドを参照してください。アクセス リストは、ローカル IP アドレスに適用され、VPN パケットが復号化される前に使用された元のクライアント IP アドレスには適用されません。

例

次に、復号化された VPN トラフィックがインターフェイス アクセス リストに従うようにする例を示します。

```
hostname(config)# no sysopt connection permit-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection preserve-vpn-flows

トンネルのドロップおよび回復後のタイムアウト期間内に、ステートフル（TCP）トンネル IPSec LAN-to-LAN トラフィックを保持して再開するには、**sysopt connection preserve-vpn-flows** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection preserve-vpn-flows

no sysopt connection preserve-vpn-flows

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

永続的 IPSec トンネル フロー機能がイネーブルの場合、タイムアウト ウィンドウ内にトンネルが再作成される限り、セキュリティ アプライアンスで元のフロー内の状態情報にアクセスできるため、データは正常に流れ続けます。

このコマンドでは、ネットワーク拡張モードを含め、IPSec LAN-to-LAN トンネルのみがサポートされます。AnyConnect/SSL VPN または IPSec リモートアクセス トンネルはサポートされません。

例

次に、トンネルがドロップされ、タイムアウト期間内に再確立された後、トンネルの状態情報が保持されてトンネル IPSec LAN-to-LAN VPN トラフィックが再開されることを指定する例を示します。

```
hostname(config)# no sysopt connection preserve-vpn-flows
```

この機能がイネーブルかどうかを確認するには、sysopt に対して show run all コマンドを入力します。

```
hostname(config)# show run all sysopt
```

結果の例は次のとおりです。説明のために、これ以降のすべての例では、preserve-vpn-flows の項目は太字になっています。

```
no sysopt connection timewait
sysopt connection tcpmss 1380
```

```
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

既存の VPN フローを再分類するには、グローバル コンフィギュレーション モードで **sysopt connection reclassify-vpn** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection reclassify-vpn

no sysopt connection reclassify-vpn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

VPN トンネルがアップになると、このコマンドによって既存の VPN フローは再分類され、暗号化が必要なフローは分解されて再作成されます。

このコマンドは、LAN-to-LAN およびダイナミック VPN についてのみ適用されます。このコマンドは EZVPN または VPN クライアント接続には影響しません。

例

次に、VPN 再分類をイネーブルにする例を示します。

```
hostname(config)# sysopt connection reclassify-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-vpn	インターフェイスのアクセス リストをチェックすることなく、IPSec トンネルから受信するすべてのパケットを許可します。

コマンド	説明
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection tcpmss

最大 TCP セグメント サイズが設定した値を超えないようにし、指定したサイズ未満にならないようにするには、グローバル コンフィギュレーション モードで **sysopt connection tcpmss** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

構文の説明

bytes	最大 TCP セグメント サイズをバイト単位で設定します（48 ～任意の最大値）。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、*bytes* を 0 に設定します。 **minimum** キーワードの場合、*bytes* は許可される最も小さい最大値を表します。
minimum	最大セグメント サイズを上書きし、*bytes* 未満にならないようにします（48 ～ 65535 バイト）。この機能は、デフォルトでディセーブルです（0 に設定）。

デフォルト

デフォルトの最大値は 1380 バイトです。minimum 機能は、デフォルトでディセーブルです（0 に設定）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ホストとサーバが最初に接続を確立するときに、両方で最大セグメント サイズを設定できます。いずれかの最大が **sysopt connection tcpmss** コマンドで設定した値を超えている場合、セキュリティ アプライアンスによって最大は上書きされ、設定した値が挿入されます。いずれかの最大が **sysopt connection tcpmss minimum** コマンドで設定した値よりも小さい場合、セキュリティ アプライアンスによって最大は上書きされ、設定した「minimum」値が挿入されます（minimum 値は、実際には許可される最も小さい最大です）。たとえば、最大サイズを 1200 バイト、最小サイズを 400 バイトに設定した場合、ホストによって最大サイズ 1300 バイトが要求されると、セキュリティ アプライアンスによってパケットは 1200 バイト（最大）を要求するように変更されます。別のホストによって最大値 300 バイトが要求されると、セキュリティ アプライアンスによってパケットは 400 バイト（最小）を要求するように変更されます。

デフォルトの 1380 バイトでは、ヘッダー情報用の余地があるため、パケット サイズの合計は 1500 バイト（イーサネットのデフォルト MTU）を超えません。次の計算を参照してください。

1380 データ + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1500 バイト

ホストまたはサーバによって最大セグメント サイズが要求されない場合、セキュリティ アプライアンスでは RFC 793 のデフォルト値である 536 バイトが有効と見なされます。

1380 よりも大きい最大サイズを設定した場合、MTU サイズ（デフォルトでは 1500 バイト）によっては、パケットがフラグメント化される場合があります。フラグメントの数が多くなると、セキュリティ アプライアンスが Frag Guard 機能を使用する場合にパフォーマンスに影響を及ぼすことがあります。最小サイズを設定すると、TCP サーバから多数の小さい TCP データ パケットがクライアントに送信されることによってサーバおよびネットワークのパフォーマンスに影響を及ぼすことを防止できます。

（注） この機能の通常の使用には推奨されませんが、syslog IPFRAG メッセージ 209001 および 209002 が発生した場合は、*bytes* 値を大きくすることができます。

例

次に、最大サイズを 1200 に、最小サイズを 400 に設定する例を示します。

```
hostname(config)# sysopt connection tcpmss 1200
hostname(config)# sysopt connection tcpmss minimum 400
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection timewait

各 TCP 接続において、最後の通常の TCP クローズ ダウン シーケンスの後に、少なくとも 15 秒の短い TIME_WAIT 状態が強制的に維持されるようにするには、グローバル コンフィギュレーション モードで **sysopt connection timewait** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合に、この機能を使用することを推奨します。

sysopt connection timewait

no sysopt connection timewait

（注） RST パケット（通常の TCP クローズ ダウン シーケンスではない）でも、15 秒の遅延がトリガーされます。セキュリティ アプライアンスでは、接続の最後のパケット（FIN/ACK または RST）を受信した後、接続を 15 秒間保持します。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスのデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後で接続が解放されます。この即時解放ヒューリスティックにより、セキュリティ アプライアンスでは、標準クローズ シーケンスと呼ばれる最も一般的なクロージング シーケンスに基づいて、高い接続レートを維持できます。ただし、一方の端が閉じ、もう一方の端が確認応答してから独自のクロージング シーケンスを開始する標準クローズ シーケンスとは異なり、同時クローズでは、トランザクションの両端がクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、即時解放によって接続の一方の側で CLOSING 状態が保持されます。多くのソケットを CLOSING 状態にすると、エンド ホストのパフォーマンスが低下する可能性があります。たとえば、一部の WinSock メインフレーム クライアントはこの動作を示し、メインフレーム サーバのパフォーマンスを低下させることが知られています。**sysopt connection timewait** コマンドを使用すると、同時クローズ ダウン シーケンスが完了するためのウィンドウが作成されます。

例

次に、timewait 機能をイネーブルにする例を示します。

```
hostname(config)# sysopt connection timewait
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。

sysopt nodnsalias

alias コマンドを使用するときに DNS A レコード アドレスを変更する DNS インスペクションをディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt nodnsalias** 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。**alias** コマンドで NAT のみを実行し、DNS パケットの変更が不要な場合に、DNS アプリケーション インスペクションをディセーブルにします。

sysopt nodnsalias {**inbound** | **outbound**}

no sysopt nodnsalias {**inbound** | **outbound**}

構文の説明

inbound	セキュリティの低いインターフェイスから **alias** コマンドで指定されるセキュリティの高いインターフェイスへのパケットの DNS レコードの変更をディセーブルにします。
outbound	**alias** コマンドで指定されるセキュリティの高いインターフェイスからセキュリティの低いインターフェイスへのパケットの DNS レコードの変更をディセーブルにします。

デフォルト

この機能は、デフォルトでディセーブルです（DNS レコード アドレス変更はイネーブルです）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

alias コマンドによって、NAT および DNS A レコード アドレスの変更が実行されます。DNS レコードの変更をディセーブルにする場合があります。

例

次に、着信パケットの DNS アドレスの変更をディセーブルにする例を示します。

```
hostname(config)# sysopt nodnsalias inbound
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に合わせて DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt noproxyarp	インターフェイスでプロキシ ARP をディセーブルにします。

sysopt noproxyarp

インターフェイスで NAT グローバル アドレスまたは VPN クライアント アドレスに対するプロキシ ARP をディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt noproxyarp** コマンドを使用します。プロキシ ARP を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

構文の説明

interface_name	プロキシ ARP をディセーブルにするインターフェイス名。

デフォルト

プロキシ ARP は、デフォルトでイネーブルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドは、VPN クライアント アドレスが内部ネットワークと重複するときに、VPN プロキシ ARP に影響を及ぼすように拡張されました。

使用上のガイドライン

既存のネットワークと重なる VPN クライアント アドレス プールがある場合、セキュリティ アプライアンスは、デフォルトにより、すべてのインターフェイス上でプロキシ ARP を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターン トラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP が不要なインターフェイスに対して **sysopt noproxyarp** コマンドを入力する必要があります。

まれに、NAT グローバル アドレスに対してプロキシ ARP をディセーブルにする場合があります。

ホストによって IP トラフィックが同じイーサネット ネットワーク上の別のデバイスに送信される場合、ホストではそのデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが IP アドレスを所有していなくても、その固有の MAC アドレスで ARP 要求に応答する場合に使用します。NAT を設定し、セキュリティ アプライアンスのインターフェイスと同じネットワーク上にあるグローバル アドレスを指定すると、セキュリティ アプライアンスによっ

てプロキシ ARP が使用されます。トラフィックがホストにアクセスできる唯一の方法は、セキュリティ アプライアンスでプロキシ ARP が使用されている場合、セキュリティ アプライアンスの MAC アドレスが宛先グローバル アドレスに割り当てられていると主張することです。

例

次に、内部インターフェイスでプロキシ ARP をディセーブルにする例を示します。

```
hostname(config)# sysopt noproxyarp inside
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に合わせて DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS A レコード アドレスの変更をディセーブルにします。

sysopt radius ignore-secret

RADIUS アカウンティング応答内の認証キーを無視するには、グローバル コンフィギュレーション モードで **sysopt radius ignore-secret** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。一部の RADIUS サーバとの互換性のために、このキーを無視する必要がある場合があります。

sysopt radius ignore-secret

no sysopt radius ignore-secret

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

一部の RADIUS サーバでは、アカウンティング確認応答内のオーセンティケータ ハッシュにこのキーが含まれていません。この使用上の注意により、セキュリティ アプライアンスでアカウンティング要求を継続的に再送信する場合があります。**sysopt radius ignore-secret** コマンドを使用して、これらの確認応答内のキーを無視し、再送信の問題を回避します （ここで示すキーは、**aaa-server host** コマンドで設定するものと同じです）。

例

次に、アカウンティング応答内の認証キーを無視する例を示します。

```
hostname(config)# sysopt radius ignore-secret
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバを指定します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。