CHAPTER 31

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

shun

新しい接続を阻止し、既存の接続からのパケットを拒否することによって、攻撃ホストへのダイナミックな応答をイネーブルにするには、特権 EXEC モードで **shun** コマンドを使用します。セキュリティ アプライアンスが排除のルックアップに使用する実際のアドレス（*src_ip*）に基づく排除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 *src_ip* [*dst_ip src_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *src_ip* [**vlan** *vlan_id*]

シンタックスの説明

dest_port	（オプション）排除を引き起こす接続の宛先ポート。
dst_ip	（オプション）ターゲット ホストのアドレス。
protocol	（オプション）UDP や TCP などの IP プロトコル。*dst_ip* を指定する場合は必須です。
src_ip	攻撃ホストのアドレス。
src_port	（オプション）排除を引き起こす接続の送信元ポート。
vlan_id	（オプション）VLAN ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

shun コマンドを使用すると、攻撃を受けるインターフェイスにブロッキング機能を適用できます。攻撃ホストの IP 送信元アドレスを含むパケットは、ブロッキング機能が手動でまたは Cisco IPS マスター モジュールによって削除されるまで、ドロップされ記録されます。IP 送信元アドレスからの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せん。残っている接続はすべて、標準アーキテクチャの一部としてタイムアウトになります。**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であるかどうかに関らず適用されます。

ホストの送信元 IP アドレスだけを指定して **shun** コマンドを使用する場合、デフォルトは 0 となります。攻撃ホストからのトラフィックは許可されません。

shun コマンドは、攻撃のダイナミックなブロックに使用されるため、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。

インターフェイスを削除すると、そのインターフェイスに適用されている排除もすべて削除されます。新しいインターフェイスを追加する場合や、同じインターフェイス（同じ名前）を置き換える場合、そのインターフェイスを IPS センサーで監視するときは、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

次の例は、攻撃ホスト（10.1.1.27）が TCP で攻撃対象（10.2.2.89）との接続を作成していることを示しています。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
```

shun コマンドを次のように適用したとします。

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

上のコマンドにより、セキュリティ アプライアンス接続テーブルから接続が削除され、10.1.1.27 からのパケットがセキュリティ アプライアンスを通過できなくなります。攻撃ホストは、セキュリティ アプライアンスの内部にある場合も、外部にある場合もあります。

関連コマンド

コマンド	説明
clear shun	現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去します。
show shun	排除情報を表示します。

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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

物理インターフェイスは、デフォルトではすべて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インターフェイスは、コンフィギュレーション内ではシャットダウンされません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**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 モードのコマンドに変更されました。

使用上のガイドライン

物理インターフェイスは、デフォルトではすべてシャットダウンされます。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト 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をシステム コンフィギュレーションでもイネーブルにする必要があります。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、そのインターフェイスを共有しているすべてのコンテキストでダウンします。

例

次の例では、メインのインターフェイスをイネーブルにしています。

```
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
```

次の例では、サブインターフェイスをイネーブルにしています。

```
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
```

次の例では、サブインターフェイスをシャットダウンしています。

```
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	既存の接続に関するすべての変換をリセットして、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 モードに入ります。

sla monitor

SLA オペレーションを作成するには、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 オペレー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。

sla monitor *sla_id*

no sla monitor *sla_id*

シンタックスの説明

sla_id	設定する SLA の ID を指定します。SLA がまだ存在しない場合は、SLA が作成されます。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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 コマンドを使用すると、SLA オペレーションを作成し、SLA モニタ コンフィギュレーション モードに入ります。このコマンドを入力すると、コマンド プロンプトが、SLA モニタ コンフィギュレーション モードに入っていることを示す `hostname(config-sla-monitor)#` に変更されます。SLA オペレーションがすでに存在していて、タイプがすでに SLA オペレーション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。最大で 2000 の SLA オペレーションを作成できます。常時デバッグ可能な SLA オペレーションは 32 だけです。

no sla monitor コマンドは、指定した SLA オペレーションとそのオペレーションの設定に使用したコマンドを削除します。

SLA オペレーションの設定後に、**sla monitor schedule** コマンドを使用してそのオペレーションのスケジュールを設定する必要があります。SLA オペレーションのコンフィギュレーションは、オペレーションのスケジュールを設定した後は修正できません。スケジュールを設定した SLA オペレーション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済みの SLA オペレーションを完全に削除する必要があります。SLA オペレーションを削除すると、関連付けられている **sla monitor schedule** コマンドも削除されます。この後に、SLA オペレーションのコンフィギュレーションを再度入力できます。

オペレーション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 オペレーションの操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 オペレーションを設定し、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 オペレーション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の設定を表示します。
sla monitor schedule	SLA オペレーションのスケジュールを設定します。
timeout	SLA オペレーションが応答を待機する期間を設定します。
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 オペレーションのスケジュ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 **sla monitor schedule** コマンドを使用します。SLA オペレーションのスケジュールの設定を削除し、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*

シンタックスの説明

after *hh*:*mm*:*ss*	コマンド入力後に、指定した時刻（時 : 分 : 秒）にオペレーションが開始されることを示します。
ageout *seconds*	（オプション）オペレーションが情報を収集していないときに、そのオペレーションをメモリに保存する秒数を指定します。SLA オペレーションは、無効になると、実行コンフィギュレーションから削除されます。
day	オペレーションを開始する日。有効値は 1 ～ 31 です。日が指定されていない場合、現在の日が使用されます。日を指定する場合、月も指定する必要があります。
hh:*mm*[:*ss*]	24 時間制で絶対開始時間を指定します。秒はオプションです。*month* と *day* を指定しない場合、次にこの指定した時間が来るとオペレーションが開始されます。
life forever	（オプション）オペレーションを無期限に実行するようにスケジュールを設定します。
life *seconds*	（オプション）オペレーションが情報を収集する秒数を指定します。
month	（オプション）オペレーションを開始する月。月が指定されない場合、現在の月が使用されます。月を指定する場合、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、最初の 3 文字だけ入力します。
now	コマンドの入力と同時に、オペレーションを開始することを示します。
pending	情報を収集しないことを示します。これはデフォルトの状態です。
recurring	（オプション）オペレーションが毎日、指定の時刻に自動的に開始し、指定の期間実行されることを示します。
sla-id	スケジュールを設定する SLA オペレーションの ID。
start-time	SLA オペレーションを開始する時間を設定します。

デフォルト

デフォルトは次のとおりです。

- SLA オペレーションは、スケジュールされた時間になるまで、***pending*** 状態です。この状態では、オペレーションはイネーブルだが、データを収集しません。
- デフォルトの ***ageout*** 時間は 0 秒です（無効になりません）。
- デフォルトの ***life*** は 3600 秒（1 時間）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	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
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 オペレーションがアクティブな状態の場合、ただちに情報を収集します。次の点線と W、X、Y、Z は、オペレーションが無効になるまでの段階を示しています。

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

- W は、**sla monitor** コマンドを使用して、SLA オペレーションを設定した時間です。
- X は、SLA オペレーションの開始時間です。ここでオペレーションは「アクティブ」になります。
- Y は、**sla monitor schedule** コマンドによって設定された有効期間の終わりを示します（***life*** 秒は 0 になります）。
- Z は、オペレーションが無効になったことを示します。

オペレーションが無効になるまでの段階として、W が開始時点で、X と Y の間は中断、Y で設定サイズにリセットされて再開されます。SLA オペレーションが無効になると、SLA オペレーション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。オペレーションは実行される前に無効になる可能性があります（つまり、Z は X の前に発生する可能性があります）。オペレーションが実行前に無効にならないようにするには、設定時間（X）と開始時間（W）の差異は、無効にならない秒数にする必要があります。

recurring キーワードは、単一の SLA オペレーションのスケジュール設定でのみ使用できます。1 回 **sla monitor schedule** コマンドを実行するだけで、複数の SLA オペレーションのスケジュールを設定することはできません。繰り返し行われる SLA オペレーションの ***life*** 値は、1 日未満にする必要があります。繰り返し行われるオペレーションの ***ageout*** 値を「無期限」（値 0 で指定）にするか、***life*** 値と ***ageout*** 値の合計を 1 日より大きい値にする必要があります。recurring オプションを指定しない場合、オペレーション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。

SLA オペレーションのコンフィギュレーションは、オペレーションのスケジュールを設定した後は修正できません。スケジュールされた SLA オペレーション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 オペレーションを完全に削除します。SLA オペレーションを削除すると、関連付けられている **sla monitor schedule** コマンドも削除されます。この後に、SLA オペレーションのコンフィギュレーションを再度入力できます。

例

次の例では、4 月 5 日午後 3:00 にデータ収集を開始するようスケジュール設定した SLA オペレーション 25 を示します。このオペレーションは、アクティブでない状態で 12 時間経過すると無効になります。この SLA オペレーションが無効になると、SLA オペレーションのすべてのコンフィギュレーション情報が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
```

次の例では、5 分間の遅延の後に、データ収集を開始するようスケジュール設定した SLA オペレーション 1 を示します。1 時間のデフォルトの有効時間が適用されます。

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

次の例では、データ収集をただちに開始し、無期限に実行するようスケジュール設定された SLA オペレーション 3 を示します。

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

次の例では、毎日午前 1:30 にデータ収集を自動的に開始するようスケジュール設定された SLA オペレーション 15 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の設定を表示します。
sla monitor	SLA 監視オペレーションを定義します。

smtps

SMTPS コンフィギュレーション モードに入るには、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 モードで入力したすべての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 接続を通じた電子メール送信を可能にする TCP/IP プロトコルです。

smtps

no smtps

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、SMTPS コンフィギュレーション モードに入る方法を示しています。

```
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。アトリビュー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。

セキュリティ アプライアンスには、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ときにイベント システムが使用できる、内部 SMTP クライアントが含まれています。これらのイベント通知を SMTP サーバで受信して、指定した電子メール アドレスに転送するように SMTP サーバを設定することができます。SMTP ファシリティ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 イベントをイネーブルにしている場合だけです。

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

no smtp-server

シンタックスの説明

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 名のいずれかを使用します。
backup_server	プライマリ SMTP サーバが使用不能になった場合に、イベント メッセージのリレー先となるバックアップ SMTP サーバを指定します。IP アドレスまたは DNS 名のいずれかを使用します。

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

次の表は、このコマンドを入力できるモードを示しています。

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

例

次の例は、SMTP サーバの IP アドレスとして 10.1.1.24 を設定し、バックアップ SMTP サーバの IP アドレスとして 10.1.1.34 を設定する方法を示しています。

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

関連コマンド

コマンド	説明

snmp-map

SNMP 検査のパラメータを定義している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*

シンタックスの説明

map_name	SNMP マップの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 コマンドは、SNMP 検査のパラメータを定義している特定のマップを指定するために使用します。このコマンドを入力すると、システムが SNMP マップ コンフィギュレーション モードに入って、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 マップを定義した後は、**inspect snmp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

例

次の例は、SNMP トラフィックを識別し、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方法を示しています。

```
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先のトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

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*]

シンタックスの説明

text	コミュニティ ストリングを設定します。

デフォルト

デフォルトのコミュニティ ストリングは **public** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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、管理されているネットワーク ノードとの間での共有秘密です。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ますが、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 アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホストの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 の連絡先名を設定するには、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。連絡先名を削除するには、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*]

シンタックスの説明

text	連絡先の担当者またはセキュリティ アプライアンスの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ます。最大 127 文字までです。スペースを使用できますが、複数のスペースは 1 つのスペースに短縮されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

例

次の例では、連絡先として Pat Johnson を設定します。

```
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 アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホストの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 アプライアンス上で 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 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、SNMP サーバはイネーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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コンフィギュレーションを設定、再設定せずに、SNMP を簡単にイネーブル / ディセーブルにできます。

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。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホストの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 アプライアンスをイネーブルにしてトラップを NMS に送信するには、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*]]

シンタックスの説明

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 トラップは次のとおりです。 • **session-threshold-exceeded**
snmp [*trap*]	SNMP トラップをイネーブルにします。デフォルトでは、SNMP トラップはすべてイネーブルです。**snmp** のトラップは次のとおりです。 • **authentication** • **linkup** • **linkdown** • **coldstart**
syslog	syslog 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、**snmp** トラップはすべてイネーブルです（**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** コマンドは、SNMP トラップをデフォルトのイネーブルに戻します。

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

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

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

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。

トラップを NMS に送信するには、**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 アプライアンス上で SNMP をイネーブルにします。
snmp-server host	SNMP ホストの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 host

セキュリティ アプライアンス上で SNMP を使用できる 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。NSM 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_name ip_address* [**trap** | **poll**] [**community** *text*] [**version** {**1** | **2c**}] [**udp-port** *port*]

no snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community** *text*] [**version** {**1** | **2c**}] [**udp-port** *port*]

シンタックスの説明

community *text*	この NMS のコミュニティ ストリングを設定します。
host	トラップが送信される NMS の IP アドレス、または SNMP 要求の送信元の NMS の IP アドレスを指定します。
interface_name	NMS がセキュリティ アプライアンスと通信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 要求の送信元である NMS の IP アドレスを指定します。
trap	（オプション）トラップのみが送信され、このホストはブラウジング（ポーリング）を実行できないことを指定します。
poll	（オプション）このホストはブラウジング（ポーリング）を実行できるが、トラップは送信されないことを指定します。
udp-port *udp_port*	（オプション）通知の送信先とする UDP ポートを設定します。SNMP トラップは、デフォルトで UDP ポート 162 を使用して送信されます。
version {**1** | **2c**}	（オプション）SNMP 通知バージョンをバージョン 1 または 2c 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

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

最大で 32 の NMS を指定できます。

例

次の例では、ホストを境界インターフェイスに接続されている 10.1.2.42 に設定します。

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

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 アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
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 要求のリッスン 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 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*

シンタックスの説明

lport	着信要求を受け入れるポート。デフォルト ポートは 161 です。[1]

1. **snmp-server** ***listen-port*** コマンドは、システム コンテキストでは使用できないため、管理テキストでのみ使用できます。

デフォルト

デフォルト ポートは 161 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

例

次の例はリッスン ポートを 192 に設定します。

```
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 アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
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 にセキュリティ 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*]

シンタックスの説明

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る最大 127 文字の値です。スペースを使用できますが、複数のスペースは 1 つのスペースに短縮されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

例

次の例では、場所を Building 42、Sector 54 として設定します。

```
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 アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホストの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 フィールドを指定するには、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**}

シンタックスの説明

mask	ソフトウェア バージョンに SIP メッセージ マスクを設定します。
log	違反が発生した場合、独自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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

次の例は SIP 検査ポリシー マップでソフトウェア バージョンを識別する方法を示します。

```
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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

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。速度の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***]

シンタックスの説明

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 パラメータはネゴシエートしないでください。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、およびこのコマンドの **no** 形式だけです。この値を **no speed nonegotiate**（デフォルト）に設定すると、インターフェイスはリンクのネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**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 モードのコマンドに変更されました。

使用上のガイドライン

速度は、物理インターフェイスに対してのみ設定します。

ネットワークが自動検出をサポートしていない場合は、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 ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度またはデュプレックス方式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方式の両方に明示的に固定値を設定して、両方の設定に関するオートネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

PoE ポートの速度を **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 とシスコの無線アクセス ポイントは検出されず給電されません。

例

次の例では、速度を 1000BASE-T に設定しています。

```
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消去します。
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 モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスの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。**split-dns none** コマンドを発行して作成されたヌル リストを含めて、設定済みのスプリット トンネリング ドメインのリストが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 グループ ポリシーに含まれているリストを継承します。ユーザがこれらのスプリット トンネリング ドメイン リストを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*]

シンタックスの説明

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の名前を提供します。
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 リストにヌル値を設定して、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されているグループ ポリシーからスプリット DNS リストを継承しないようにします。

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

次の表は、このコマンドを入力できるモードを示しています。

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

ドメインのリストに記述する各エントリは、1 個のスペースを使用して区切ります。エントリの数に制限はありませんが、エントリ文字列の長さは、255 文字を超えることはできません。使用できるのは、英数字、ハイフン（-）、およびピリオド（.）のみです。

no spilit-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されたヌル値を含めて、現在の値がすべて削除されます。

例

次の例は、FirstGroup というグループ 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 を設定する方法を示しています。

```
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 フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトの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-tunnel-network-list

スプリット トンネリング用のネットワークの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。ネットワークの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 ネットワークの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。**split-tunnel-network-list none** コマンドを発行して作成されたヌル リストを含めて、設定済みのネットワーク リストがすべて削除されます。

スプリット トンネリング ネットワークのリストがない場合、ユーザは、デフォルト グループ ポリシーまたは指定したグループ ポリシーに含まれているネットワーク リストを継承します。ユーザがこれらのネットワーク リストを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 ネットワークのリストは、トラフィックにトンネルの通過を要求するネットワークと、トンネリングを要求しないネットワークとを区別するためのものです。

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

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

シンタックスの説明

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したアクセス リストを指定します。
none	スプリット トンネリング用のネットワークのリストが存在しないことを指定します。セキュリティ アプライアンスは、すべてのトラフィックをトンネリングします。 スプリット トンネリング ネットワークのリストにヌル値を設定して、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されているグループ ポリシーから、スプリット トンネリング ネットワークのデフォルトのリストを継承しないようにします。

デフォルト

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

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

セキュリティ アプライアンスは、スプリット トンネリングを実行するかどうかをネットワーク リストに基づいて判断します。このリストは、プライベート ネットワーク上にあるアドレスのリストで構成される、標準的な ACL です。

no spilit-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されたヌル値を含めて、現在のネットワーク リストがすべて削除されます。

例

次の例は、FirstGroup というグループ ポリシーに対して、FirstList というネットワーク リストを設定する方法を示しています。

```
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 リストを作成します。または、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 フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトの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-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。split-tunnel-policy のアトリビュートを実行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。このコマンドを使用すると、スプリット トンネリングの値を別のグループ ポリシーから継承できます。

スプリット トンネリングを利用すると、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 トンネリングがイネーブルになっている場合、宛先が IPSec トンネルの向こう側ではないパケットについては、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が不要です。

このコマンドは、このようなスプリット トンネリング ポリシーを特定のネットワークに適用するものです。

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

no split-tunnel-policy

シンタックスの説明

excludespecified	トラフィックを暗号化なしで送信する宛先ネットワークのリストを定義します。この機能が役立つのは、企業ネットワークにトンネル経由で接続しながら、ローカル ネットワーク上のプリンタなどのデバイスにアクセスしようとするリモート ユーザです。このオプションが適用されるのは、Cisco VPN Client のみです。
split-tunnel-policy	トラフィックのトンネリング規則を設定することを指定します。
tunnelall	トラフィックを暗号化なしでは送信しないこと、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 ネットワークには企業ネットワークを通じて到達し、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のトラフィック、または指定したネットワークに向かうトラフィックをすべてトンネリングします。このオプションを指定すると、スプリット トンネリングがイネーブルになります。これによって、トンネリングの対象となるネットワークのアドレス リストを作成できるようになります。他のアドレス宛てのデータは、すべて暗号化なしで送信され、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

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

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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お勧めします。

例

次の例は、FirstGroup というグループ ポリシーに対して、指定したネットワークのみ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方法を示しています。

```
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 フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトの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 トンネリング用のアクセス リストが存在し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 プロトコル検査のために、サーバ ヘッダー フィールドの文字列を置き換えるには、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*

シンタックスの説明

string	サーバ ヘッダー フィールドに代入する文字列。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

次の表は、このコマンドを入力できるモードを示しています。

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

次の例では、HTTP 検査ポリシー マップでサーバ ヘッダー フィールドの文字列を置き換える方法を示します。

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

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

ssh

セキュリティ アプライアンスへの 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 アドレスと IPv6 アドレスをサポートしています。

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

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

シンタックスの説明

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 SSH が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 接続の開始が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 接続の開始が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

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

ssh *ip_address* コマンドは、セキュリティ アプライアンスへの SSH 接続の開始を認可す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** 形式は、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。

SSH を使用してセキュリティ アプライアンスに接続するには、**crypto key generate rsa** コマンドを使用して、デフォルトの RSA キーをあらかじめ生成しておく必要があります。

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 暗号と AES 暗号
- パケットの完全性を保証するための HMAC-SHA アルゴリズムと 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

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

- X11 転送
- ポート転送
- SFTP サポート
- Kerberos と AFS のチケットの引き渡し
- データ圧縮

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 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 コマンドを消去します。
crypto key generate rsa	ID 証明書のための 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内の現在の SSH コマンドを表示します。
ssh scopy enable	セキュリティ アプライアンス上でセキュア コピー サーバをイネーブルにします。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

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*

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

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

次の例は、SSH セッションが切断される様子を示しています。

```
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 アプライアンス上のアクティブな 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 アプライアンス上でセキュア コピー（SCP）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

シンタックスの説明

このコマンドには、キーワードも引数もありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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、サーバ専用の実装です。SCP のための接続を受け入れること、および終了することはできますが、開始することはできません。セキュリティ アプライアンスでは、次の制限事項があります。

- SCP のこの実装では、ディレクトリをサポートしていないため、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 アクセスだけを実行できます。
- SCP 使用時は、バナーをサポートしていません。
- SCP はワイルドカードをサポートしません。
- 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 機能が含まれている必要があります。

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 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 コマンドを消去します。
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内の現在の 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	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

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

シンタックスの説明

number	SSH セッションが切断されるまでに非アクティブ状態を維持する時間（分）を指定します。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

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

ssh timeout コマンドは、セッションが切断されるまでにアイドル状態を維持する時間（分）を指定します。デフォルトの時間は 5 分です。

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 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 コマンドを消去します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
show ssh sessions	セキュリティ アプライアンス上のアクティブな 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*]

シンタックスの説明

1	SSH バージョン 1 接続のみをサポートすることを指定します。
2	SSH バージョン 2 接続のみをサポートす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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 と 2 は、セキュリティ アプライアンスが使用する SSH のバージョンをいずれかに限定するように指定します。このコマンドの **no** 形式は、セキュリティ アプライアンスをデフォルトの状態である互換モード（両方のバージョンを使用可能）に戻します。

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 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 コマンドを消去します。
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内の現在の 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 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ときに使用する 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 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** 形式を使用します。このコマンドを使用すると、セキュリティ アプライアンスが送信する 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

シンタックスの説明

any	セキュリティ アプライアンスは、SSL バージョン 3 の hello を送信し、SSL バージョン 3 または TLS バージョン 1 のいずれかをネゴシエートします。
sslv3-only	セキュリティ アプライアンスは、SSL バージョン 3 の hello を送信し、SSL バージョン 3 のみを受け入れます。
tlsv1-only	セキュリティ アプライアンスは、TLS バージョン 1 クライアントの hello を送信し、TLS バージョン 1 のみを受け入れます。

デフォルト

デフォルト値は、**any** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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)(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 ポート転送は、WebVPN ユーザが一部の SSL バージョンを使用して接続している場合には機能しません。次に説明を示します。

Negotiate SSLv3	Java がダウンロードされる
Negotiate SSLv3/TLSv1	Java がダウンロードされる
Negotiate TLSv1	Java がダウンロードされない
TLSv1Only	Java がダウンロードされない
SSLv3Only	Java がダウンロードされない

問題となるのは、ポート転送アプリケーションを起動したときに、Java はクライアントの Hello パケットで SSLv3 のみをネゴシエートする点です。

例

次の例は、SSL クライアントとして動作するときに、TLSv1 だけ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方法を示しています。

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

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
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	セキュリティ アプライアンスがサーバとして動作するときに使用する、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。このコマンドをもう一度発行すると、直前の設定が上書きされます。アルゴリズムを使用する優先順位は、アルゴリズムの順序によって決まります。アルゴリズムを追加または削除して、使用している環境での要件を満たすようにしてください。デフォルト（すべての暗号化アルゴリズムが使用可能）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

シンタックスの説明

3des-sha1	Secure Hash Algorithm 1 を使用する Triple 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 Triple 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 Triple AES 256 ビット暗号化を指定します。
possibly others	暗号化アルゴリズムが、将来のリリースで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が次の順序で使用可能になっています。

[*3des-sha1***] [***des-sha1***] [***rc4-md5***] [***possibly others***]**

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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)(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 タブでは、設定する値ではなく、ライセンスがサポートする暗号化の最大レベルが反映されます。

例

次の例は、3des-sha1 暗号化アルゴリズムと 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方法を示しています。

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

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
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	セキュリティ アプライアンスがサーバとして動作するときに使用する、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

セキュリティ アプライアンスがサーバとして動作するときに使用する 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** 形式を使用します。このコマンドを使用すると、セキュリティ アプライアンスが受け入れる 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

シンタックスの説明

any	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、SSL バージョン 3 または TLS バージョン 1 のいずれかをネゴシエートします。
sslv3	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、SSL バージョン 3 をネゴシエートします。
sslv3-only	セキュリティ アプライアンスは、SSL バージョン 3 クライアントの hello のみを受け入れ、SSL バージョン 3 のみを使用します。
tlsv1	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、TLS バージョン 1 をネゴシエートします。
tlsv1-only	セキュリティ アプライアンスは、TLSv1 クライアントの hello のみを受け入れ、TLS バージョン 1 のみを使用します。

デフォルト

デフォルト値は、**any** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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)(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 ポート転送は、WebVPN ユーザが一部の SSL バージョンを使用して接続している場合には機能しません。次に説明を示します。

Negotiate SSLv3	Java がダウンロードされる
Negotiate SSLv3/TLSv1	Java がダウンロードされる
Negotiate TLSv1	Java がダウンロードされない
TLSv1Only	Java がダウンロードされない
SSLv3Only	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は、SSL バージョンを tlsv1-only に設定しないでください。Outlook と Outlook Express は、TLS をサポートしていません。

例

次の例は、SSL サーバとして動作するときに、TLSv1 だけ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方法を示しています。

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

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
show running-config ssl	現在設定されている ssl コマンドのセットを表示します。
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に使用される、フォールバック トラストポイントが作成されます。インターフェイスの指定がない 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。インターフェイスの指定がない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

シンタックスの説明

interface	トラストポイントを適用するインターフェイス名。このインターフェイス名は、**nameif** コマンドで指定したものです。
trustpoint	**crypto ca trustpoint** {*name*} コマンドで設定した、CA トラストポイントの *name*。

デフォルト

トラストポイントの関連付けはありません。セキュリティ アプライアンスは、デフォルトの自己生成 RSA キー ペア証明書を使用します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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)(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場合は、次の注意事項に従ってください。

- *trustpoint* の値は、**crypto ca trustpoint {*name*}** コマンドで設定した CA トラストポイントの名前にする必要があります。
- *interface* の値は、事前設定済みのインターフェイスの *nameif* 名にする必要があります。
- 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している **ssl trust-point** エントリもすべて削除されます。
- **ssl trustpoint** エントリは、インターフェイスごとに 1 つずつ、およびインターフェイスの指定がないもの 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。

次の例は、このコマンドの **no** 形式を使用する方法を示しています。

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

次の例は、内部インターフェイス用の FirstTrust という SSL トラストポイント、および関連するインターフェイスを持たない DefaultTrust というトラストポイントを設定する方法を示しています。

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

次の例は、このコマンドの **no** 形式を使用して、関連するインターフェイスを持たないトラストポイントを削除する方法を示しています。

```
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
```

次の例は、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方法を示しています。

```
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	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
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	セキュリティ アプライアンスがサーバとして動作するときに使用する、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シングル サインオン サーバを作成するには、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。これは CA SiteMinder コマンドによる SSO です。

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*

no sso-server *name* **type** *siteminder*

（注）　SSO 認証にはこのコマンドが必要です。

シンタックスの説明

name	SSO サーバの名前を指定します。文字数は最小 4 文字から最大 31 文字までです。
siteminder	セキュリティ アプライアンスは CA SiteMinder と互換性があるため、使用できる引数は *siteminder* だけです。
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 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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。**sso-server** コマンドを使用して SSO サーバを作成できます。SSO サーバを作成したら、認証 URL（**web-agent-url** コマンドを参照）、およびサーバとのコミュニケーションを保護するための秘密鍵（**policy-server-secret** コマンドを参照）を任意の順序で設定する必要があります。

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。現在、セキュリティ アプライアンスは、Computer Associates の eTrust SiteMinder SSO サーバ（以前の Netegrity SiteMinder）をサポートしています。したがって、タイプのオプションに使用できる引数は *siteminder* です。

例

webvpn コンフィギュレーション モードで入力した次の例では、「example」という名前の SSO サーバを作成しています。

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

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
request-timeout	失敗した SSO 認証試行が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 サーバの動作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。
web-agent-url	セキュリティ アプライアンスが 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 コンフィギュレーション）

グループ ポリシーに SSO サーバを割り当てるには、グループ ポリシーの 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。これは CA SiteMinder コマンドによる SSO です。

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 ポリシーを継承し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*

シンタックスの説明

name	グループ ポリシーに割り当てられる 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たデフォルト ポリシーは DfltGrpPolicy です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループの 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 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。グループ ポリシーの 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。

（注） 同じコマンド（**sso-server value**）をユーザ名の webvpn コンフィギュレーション モードで入力すると、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。

例

次の例は、コマンドによって my-sso-grp-pol という名前のグループ ポリシーを作成し、そのグループ ポリシーを example という名前の SSO サーバに割り当てます。

```
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	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
show webvpn sso-server	SSO サーバの動作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** コンフィギュレーション）	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 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 コンフィギュレーション）

ユーザ ポリシーに SSO サーバを割り当てるには、ユーザ名 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。これは CA SiteMinder コマンドによる SSO です。

ユーザへの 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た場合は、**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*

シンタックスの説明

name	ユーザ ポリシーに割り当てられる 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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名の 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 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。**sso-server value** コマンドを使用すると、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）　同じコマンド（**sso-server value**）をグループの webvpn コンフィギュレーション モードで入力すると、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。

例

次のコマンドの例では、my-sso-server という名前の SSO サーバを、Anyuser というユーザ名の WebVPN ユーザのユーザ ポリシーに割り当てています。

```
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	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
show webvpn sso-server	SSO サーバの動作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（グループ ポリシー webvpn コンフィギュレーション）	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 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 クッキーを取得する 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** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

start-url *string*

（注）　HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

string	SSO サーバの URL です。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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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、認証 Web サーバにシングル サインオン認証要求を送信するために HTTP POST 要求を使用できます。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共に送信することにより、事前ログイン シーケンスを実行できます。ブラウザで認証 Web サーバのログイン ページに直接接続すると、この実行を検出できます。ログイン ページがロードされるときに Web サーバがクッキーを設定し、そのクッキーが次のログイン セッションに関連している場合は、クッキーが取得される URL に入るために **start-url** コマンドを使用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提出により開始されます。

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

例

AAA サーバ ホスト コンフィギュレーション モードで入力された次の例では、https://example.com/east/Area.do?Page-Grp1 の事前ログイン クッキーを取得するための URL を指定しています。

```
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とパスワードを受信する 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 サーバとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求の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]

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

次の例は、H.323 コールで RAS の状態チェックを実行する方法を示しています。

```
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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

static

実際の IP アドレスをマッピング 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 のアドレス変換規則を設定するには、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* {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name* | **interface**} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

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

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

シンタックスの説明

access-list *access_list_name*	実際のアドレスと宛先アドレス（またはポート）を指定して、NAT 用の実際のアドレスを指定できます。この機能は、ポリシー NAT と呼ばれます。 アクセス リストで使用されるサブネット マスクは、*mapped_ip* でも使用されます。 アクセス リストには、**permit** 文だけを含めることができます。**eq** 演算子を使用して、実際のポートと宛先ポートをアクセス リスト内で指定することもできます。ポリシー NAT の場合、**inactive** キーワードと **time-range** キーワードは考慮されません。ポリシー NAT の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ものと見なされます。
dns	（オプション）DNS 応答に含まれていて、このスタティック エントリと一致する A レコード（アドレス レコード）を書き換えます。マッピングされているインターフェイスから実際のインターフェイスに移動する DNS 応答では、A レコードが、マッピングされた値から実際の値に書き直されます。逆に、実際のインターフェイスからマッピングされているインターフェイスに移動する DNS 応答では、A レコードが、実際の値からマッピングされた値に書き直されます。 **（注）** この機能をサポートするには、DNS 検査をイネーブルにする必要があります。
emb_lim	（オプション）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。

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。このキーワードを使用するのは、インターフェイス アドレスを使用しようとする場合に、アドレスが DHCP を使用して動的に割り当てられているときです。 **（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のではなく、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	実際のアドレスの変換後のアドレスを指定します。
mapped_port	マッピング TCP ポートまたは UDP ポートを指定します。ポートは、リテラル名または番号（0 ～ 65535）のどちらでも指定できます。 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	（オプション）非対称ルーティング トラフィックの TCP セッションを許容します。このオプションを指定すると、着信トラフィックは、対応する発信接続の状態が確立されていなくてもセキュリティ アプライアンスを通過することができます。**failover timeout** コマンドと共に使用します。**failover timeout** コマンドは、システムがブートしたときまたはアクティブになったときを起点として、ネイリングされたセッションが受け入れられる期間を指定するものです。設定しない場合は、接続を再確立できません。 **（注）** **static** コマンドに ***nailed*** オプションを付加すると、当該の接続については TCP の状態追跡とシーケンス確認が省略されます。非対称ルーティングのサポートを設定する場合は、**asr-group** コマンドを使用する方が **static** コマンドに ***nailed*** オプションを付加して使用するよりもセキュリティ上安全であり、非対称ルーティングのサポートの設定にはこの方法をお勧めします。
netmask *mask*	実際のアドレスとマッピング 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。マスク後のホストビットが 0 でない場合は、ホスト マスクの 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と、アクセス リストで使用されるサブネット マスクが *mapped_ip* にも使用されます。

norandomseq	（オプション）TCP ISN のランダム化保護をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの ISN があります。1 つはクライアントが生成し、1 つはサーバが生成します。セキュリティ アプライアンスは、ホストとサーバが生成する ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。 **norandomseq** キーワードは外部 NAT に適用されません。ファイアウォールは、セキュリティの高いインターフェイスのホスト / サーバが生成する ISN だけをランダム化します。外部 NAT に対して **norandomseq** を設定しても、**norandomseq** キーワードは無視されます。
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際の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。ポートは、リテラル名または番号（0 ～ 65535）のどちらでも指定できます。 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 の場合に、プロトコルを TCP として指定します。
tcp *max_conns*	サブネット全体に関して、同時 TCP 接続の最大数を指定します。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）。
udp	スタティック PAT の場合に、プロトコルを UDP として指定します。
udp *udp_max_conns*	（オプション）サブネット全体に関して、同時 UDP 接続の最大数を指定します。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）。

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

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

スタティック NAT では、実際のアドレス（複数可）からマッピング アドレス（複数可）への固定的な変換を作成します。ダイナミック NAT およびダイナミック PAT の場合、後続の変換では、各ホストはそれぞれ別の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、マッピング アドレスは連続する各接続で同じであり、恒久的な変換規則が存在します。このため、スタティック NAT を利用する場合は、宛先ネットワーク上のホストが変換後のホストに向かうトラフィックを開始できます（この処理を許可するアクセス リストが存在する場合）。

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 を利用する場合、変換後のホストに向かう接続をリモート ホストが開始できることです（この処理を許可するアクセス リストが存在する場合）。ダイナミック NAT の場合はできません。また、スタティック NAT では、実際のアドレスと同じ数のマッピング アドレスが必要になります。

スタティック PAT はスタティック NAT と同じですが、実際のアドレスおよびマッピング アドレスに対して、プロトコル（TCP または UDP）と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、同じマッピング アドレスを複数のさまざまな static 文に対して指定できます。ただし、それぞれの文でポートが異なっている必要があります（複数のスタティック NAT 文に対して同じマッピング アドレスを使用することはできません）。

同じ実際のアドレスまたはマッピング アドレスを、複数の **static** コマンド内で同じ 2 つのインターフェイスに関して使用することはできません。同じマッピング 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 アドレスは、**static** コマンドの中では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検査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。

NAT は、従来の意味では、透過ファイアウォール モードで使用できません。透過ファイアウォール モードでは、***static*** コマンドを使用することによって、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。この場合、実際の IP アドレスとマッピング IP アドレスは両方とも同じです。

別の方法として、**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 ランダム化を設定できます。同じトラフィックに対して両方の方法でこれらの設定値を設定した場合、セキュリティ アプライアンスは小さい方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、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。

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 コマンド文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消去してください。

例

スタティック NAT の例

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 アドレスに変換される 1 つの実際の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）にマッピングしています。

```
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 IP アドレス（209.165.201.15）を内部 IP アドレス（10.1.1.6）にマッピングしています。

```
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ています。

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

次の例は、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方法を示しています。**static** コマンドでは、アドレス 209.165.201.0 ～ 209.165.201.30 がローカル アドレス 10.1.1.1 ～ 10.1.1.30 にマッピングされます（209.165.201.1 は 10.1.1.1 にマッピングされ、209.165.201.10 は 10.1.1.10 にマッピングされ、他も同様にマッピングされます）。

```
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の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** コマンドでグローバル アドレスをセットアップして、外部のホストが dmz1 インターフェイス上の 10.1.1.1 メール サーバ ホストにアクセスすることを許可します。DNS 用の MX レコードが 209.165.201.1 アドレスを指すように設定する必要があり、これによってメールはこのアドレスに送信されます。**access-list** コマンドによって、外側ユーザが SMTP ポート（25）を経由して、グローバル アドレスにアクセスできるようにしています。**no fixup protocol** コマンドにより、Mail Guard が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開始されてセキュリティ アプライアンスの外部インターフェイス（10.1.2.14）に向かう Telnet トラフィックは、次のコマンドを入力することで内部のホスト（10.1.1.15）に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 eq telnet
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開始されてセキュリティ アプライアンスの外部インターフェイス（10.1.2.14）に向かう HTTP トラフィックは、次のコマンドを入力することで内部のホスト（10.1.1.15）に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 eq http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

セキュリティ アプライアンスの外部インターフェイス（10.1.2.14）からの Telnet トラフィックを内部ホスト 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
```

上の実際の Telnet サーバが接続を開始することを許可するには、変換を追加する必要があります。たとえば、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。元のままの **static** コマンドは、このサーバに向かう Telnet に関する変換を定義しています。それに対して、**nat** コマンドと **global** コマンドでは、このサーバからの発信接続に関する PAT を定義しています。

```
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独自の変換を定義していて、内部ホストが Telnet サーバとは別のマッピング アドレスを使用している場合でも、Telnet サーバから開始されるトラフィックについては、サーバに向かう Telnet トラフィックを許可する **static** 文と同じマッピング アドレスを使用するように設定することができます。Telnet サーバにだけ適用する、より限定的な **nat** コマンドを作成する必要があります。**nat** 文は、最もよく一致しているものが読み取られます。このため、限定的な **nat** コマンドは汎用の文よりも先に一致します。次の例は、Telnet に関する **static** 文、Telnet サーバから開始されるトラフィックに関する限定的な **nat** 文、および別のマッピング アドレスを使用するその他の内部ホストに関する文を示しています。

```
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
```

既知のポート（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	すべての変換を消去します。
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に含まれているすべての **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**}

シンタックスの説明

drop	違反が発生した場合、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、独自または追加のログを記録することを指定します。このアクションは、任意のアクションに関連付けることができます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

次の例では、SIP 検査ポリシー 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方法を示します。

```
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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

strict-http

HTTP に準拠し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。この機能の動作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。

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

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

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクション。
allow	メッセージを許可します。
drop	接続を終了します。
log	（オプション）syslog を生成します。
reset	クライアントとサーバに TCP リセット メッセージを送信して、接続を終了します。

デフォルト

このコマンドは、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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 検査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 に準拠しないトラフィックの転送をセキュリティ アプライアンスで許可することができます。このコマンドは、デフォルトの動作（HTTP に準拠しないトラフィックの転送を拒否）を上書きします。

例

次の例では、HTTP に準拠しないトラフィックの転送を許可しています。

```
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先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

strip-group

このコマンドが適用されるのは、user@realm の形式で受信したユーザ名のみです。レルムは、@ デリミタを使用してユーザ名に付加される管理ドメインです（たとえば、juser@abc）。

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 グループ一般アトリビュート モードで **strip-group** コマンドを使用します。セキュリティ アプライアンスは、VPN クライアントが提示するユーザ名からグループ名を取得して、IPSec 接続用のトンネル 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 アプライアンスは、ユーザ名のユーザ部分だけを認可と認証用に送信します。これ以外の場合（ディセーブルにした場合）、セキュリティ アプライアンスはレルムを含めて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

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトでは、このコマンドの設定はディセーブルになっています。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン　このアトリビュートは、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

次の例では、IPSec リモートアクセス タイプ用に「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、次に一般コンフィギュレーション モードに入って、「remotegrp」という名前のトンネル グループをデフォルト グループ ポリシーとして設定し、次にこのトンネル グループについてグループ除去をイネーブルにしています。

```
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
hostname(config-tunnel-general)
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
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 グループの一般アトリビュートを指定します。

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 グループ一般アトリビュート 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。レルム除去処理は、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を削除するものです。レルムは、@　デリミタを使用してユーザ名に付加される管理ドメインです（たとえば、username@realm）。このコマンドをイネーブルにすると、セキュリティ アプライアンスは、ユーザ名のユーザ部分だけを認可と認証用に送信します。ディセーブルにした場合には、セキュリティ アプライアンス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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、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

次の例では、IPSec リモートアクセス タイプ用に「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、次に一般コンフィギュレーション モードに入って、「remotegrp」という名前のトンネル グループをデフォルト グループ ポリシーとして設定し、次にこのトンネル グループについてレルム除去をイネーブルにしています。

```
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	設定されたすべてのトンネル グループまたは指定されたトンネル グループを消去します。
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 グループの一般アトリビュートを指定します。

subject-name（暗号 CA 証明書マップ）

規則エントリを IPSec ピア証明書のサブジェクト DN に適用することを指定するには、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*

シンタックスの説明

attr tag	証明書 DN にある、指定したアトリビュート値のみを規則エントリ文字列と比較することを指定します。タグの値を次に示します。 DNQ = DN 修飾子 GENQ = 世代修飾子 I = イニシャル GN = 名 N = 名前 SN = 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 = 役職 O = 組織名 L = 地名 SP = 州または都道府県 C = 国または地域 OU = 組織ユニット CN = 通常名
co	規則エントリ文字列が、DN 文字列または指定されているアトリビュートのサブストリングになる必要があることを指定します。
eq	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致する必要があることを指定します。
nc	規則エントリ文字列が、DN 文字列または指定されているアトリビュートのサブストリングにならない必要があることを指定します。
ne	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致しない必要があることを指定します。
string	一致するかどうかの確認対象となる値を指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

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

次の例では、証明書マップ 1 の CA 証明書マップ モードに入って、証明書サブジェクト名の Organization アトリビュートが Central と等しくなる必要があると指定する規則エントリを作成しています。

```
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 モードに入ります。
issuer-name	規則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** コマンドで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（暗号 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、暗号 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物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

シンタックスの説明

X.500_name	X.500 認定者名（たとえば、cn=crl,ou=certs,o=CAName,c=US）を定義します。最大長は 1,000 文字（実質上の無制限）です。

デフォルト

デフォルトでは、サブジェクト名を含めない設定になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入って、URL https//:frog.phoobin.com での自動登録をセットアップし、サブジェクト DN OU tiedye.com をトラストポイント central の登録要求に含めています。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://frog.phoobin.com/
hostname(ca-trustpoint)# subject-name ou=tiedye.com
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 モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment url	CA への登録用の URL を指定します。

summary-address

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*]

シンタックスの説明

addr	一定範囲のアドレスに指定されたサマリー アドレスの値。
mask	サマリー ルートに使用される IP サブネット マスク。
not-advertise	（オプション）指定されたプレフィックスとマスクのペアに一致するルートを抑止します。
tag *tag_value*	（オプション）各外部ルートに対応付けられた 32 ビットの 10 進値。この値は、OSPF 自体によって使用されることはありません。ASBR 間で情報を交換するために使用されます。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。有効な値は 0 ～ 4294967295 です。

デフォルト

デフォルトは次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックスとマスクのペアに一致するルートは、抑止されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

他のルーティング プロトコルからラーニングしたルートは、要約することができます。このコマンドを OSPF に対して使用すると、OSPF 自律システム境界ルータ（ASBR）は、当該アドレスの対象となる再配布されるすべてのルートの要約として、1 つの外部ルートをアドバタイズします。このコマンドが要約するのは、他のルーティング プロトコルからラーニングした、OSPF に再配布されているルートのみです。OSPF エリア間の経路集約には、**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 形式を他のオプション キーワードや引数を指定せずに使用します。オプションをコンフィギュレーション内の summary コマンドから削除するには、削除するオプションを付加してこのコマンドの **no** 形式を使用します。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 に設定して経路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)#
```

次の例は、デフォルト値に戻す対象オプションを指定して **summary-address** コマンドの **no** 形式を使用する方法を示しています。この例では、前の例で 3 に設定した *tag* の値を **summary-address** コマンドから削除しています。

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

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

```
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	エリアの境界でルートを統合および要約します。
router ospf	ルータ コンフィギュレーション モードに入ります。
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。

sunrpc-server

SunRPC サービス テーブル内に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*

シンタックスの説明

ifc_name	サーバの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*	（オプション）SunRPC プロトコルのポート範囲を指定します。
protocol tcp	SunRPC 転送プロトコルを指定します。
protocol udp	SunRPC 転送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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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、タイムアウトで指定した期間中に、SunRPC トラフィックが確立済み SunRPC セッションに基づいてセキュリティ アプライアンスを通過することを許可するために使用します。

例

次の例は、SunRPC サービス テーブルを作成する方法を示しています。

```
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 Sun リモート プロセッサ コール サービスを消去します。
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 に認証されている場合に、リモート ユーザ証明書をそのトラストポイントに基づいて検証するには、暗号 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、ユーザ証明書の検証をサポートするように設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 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。このため、同じ CA から 2 つの異なる ID 証明書が発行されることがあります。ある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 の認証を受ける場合、このオプションは自動的にディセーブルになります。したがって、パス検証パラメータの選択であいまいさが生じることはありません。ある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 の認証を受けた場合は、ユーザが当該トラストポイント上でこの機能をアクティブにしようとしても、その操作は許可されません。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

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入って、トラストポイント central でのユーザ検証の受け入れをイネーブルにしています。

```
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 モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。

svc

特定のグループまたはユーザの SVC をイネーブルにするか、または要求するには、グループ ポリシーまたはユーザ名の webvpn モードで **svc** コマンドを使用します。

コンフィギュレーションから **svc** 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 {**none** | **enable** | **required**}

no svc

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。

シンタックスの説明

none	このグループまたはユーザの SVC をディセーブルにします。
enable	このグループまたはユーザの SVC をイネーブルにします。
required	このグループまたはユーザには SVC が必要です。

デフォルト

デフォルトは **none** です。SVC はグループ ポリシーまたはユーザ ポリシーでディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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、SVC を必要とするように既存のグループ ポリシー *sales* を設定しています。

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

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについての情報を表示します。
svc enable	SVC ファイルをリモート コンピュータにダウンロードするためにセキュリティ アプライアンスをイネーブルにします。
svc image	セキュリティ アプライアンスが SVC ファイルをフラッシュ メモリから RAM にロードするように指定し、さらにセキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定します。

svc compression

特定のグループまたはユーザの SVC 接続で、http データの圧縮をイネーブルにするには、グループ ポリシーまたはユーザ名の webvpn 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 **svc compression** 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**}

シンタックスの説明

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	グループまたはユーザに対して圧縮をディセーブルにすることを指定します。

デフォルト

デフォルトでは、SVC 圧縮は *deflate*（イネーブル）に設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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

SVC 接続では、グローバル コンフィギュレーション モードで設定された **compression** コマンドが、グループ ポリシーまたはユーザ名の webvpn モードで設定された **svc compression** コマンドを上書きします。

例

次の例では、グループ ポリシー sales の SVC 圧縮はディセーブルになっています。

```
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 SVC 接続、WebVPN 接続、および IPSec VPN 接続に対して圧縮をイネーブルにします。
show webvpn svc	SVC インストレーションについての情報を表示します。

svc dpd-interval

セキュリティ アプライアンスの DPD をイネーブルにして、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定するには、グループ ポリシー またはユーザ名の 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。

シンタックスの説明

gateway *seconds*	セキュリティ アプライアンスが DPD を実行する間隔を 30 ～ 3,600 秒の範囲で指定します。
gateway none	セキュリティ アプライアンスが実行する DPD をディセーブルにします。
client *seconds*	SVC が DPD を実行する間隔を 30 ～ 3,600 秒の範囲で指定します。
client none	SVC が実行する DPD をディセーブルにします。

デフォルト

デフォルトは none です。SVC およびセキュリティ アプライアンスの DPD はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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、既存の Sales という名前のグループ ポリシーに対して、セキュリティ アプライアンス（ゲートウェイ）が実行する DPD の間隔を 3,000 秒に設定し、クライアントが実行する DPD の間隔を 1,000 秒に設定しています。

```
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 SVC をイネーブルまたは必須にします。
svc keepalive	リモート コンピュータの SVC が、セキュリティ アプライアンスにキープアライブ メッセージを送信する頻度を指定します。
svc keep-installer	リモート コンピュータへの SVC の永続的なインストールをイネーブルにします。
svc rekey	SVC セッションで SVC がキーの再生成を実行することをイネーブルにします。

svc enable

セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードすることをイネーブルにするには、webvpn 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 **svc enable** 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

デフォルトでは、このコマンドはディセーブルになっています。セキュリティ アプライアンスは SVC ファイルをダウンロードしません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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 SVC セッションは終了しません。

例

次の例では、セキュリティ アプライアンスによる SVC ファイルのダウンロードをイネーブルにしています。

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

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについて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 SVC をイネーブルまたは必須にします。
svc image	セキュリティ アプライアンスが SVC ファイルをフラッシュ メモリから RAM にロードするように指定し、さらにセキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定します。

svc image

セキュリティ アプライアンスが SVC ファイルをフラッシュ メモリから RAM にロードするように指定し、さらにセキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定するには、webvpn 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 **svc image** 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*

no svc image *filename order*

シンタックスの説明

filename	SVC ファイルのファイル名を最大 255 文字で指定します。
order	ファイル間の相対的な位置を示す番号を 1 ～ 65,535 の間で指定します。

デフォルト

デフォルトの順序は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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

SVC ファイルに番号を付けると、セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序が確立されます。セキュリティ アプライアンスは、最も小さい番号の SVC ファイルを最初にダウンロードします。したがって、オペレーティング システムで最も一般的に使用されるファイルに最小の番号を割り当てる必要があります。

ファイルは任意の順序で設定できます。たとえば、2 を 1 の前に設定することが可能です。

例

次の例で、**show webvpn svc** コマンドの出力は、windows.pkg ファイルが順序番号 1、windows2.pkg ファイルが順序番号 15 であることを示しています。リモート コンピュータが SVC 接続を確立しようとすると、windows.pkg ファイルが最初にダウンロードされます。ファイルがオペレーティング システムに一致しない場合は、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、**svc image** コマンドを使用して SVC アーカイブ ファイルの順序を変更し、リモート PC に最初にダウンロードされるファイルを windows2.pkg ファイルとして、2 番目にダウンードされるファイルを windows.pkg としています。

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

show webvpn svc コマンドを再度入力すると、新しい順序でファイルが表示されます。

```
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
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについて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 SVC をイネーブルまたは必須にします。
svc enable	SVC ファイルをリモート コンピュータにダウンロードするためにセキュリティ アプライアンスをイネーブルにします。

svc keepalive

リモート コンピュータの SVC が、セキュリティ アプライアンスにキープアライブ メッセージを送信する頻度を設定するには、**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 keepalive {**none** | *seconds*}

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

シンタックスの説明

none	SVC のキープアライブ メッセージをディセーブルにします。
seconds	SVC がキープアライブ メッセージを送信することをイネーブルにし、15 ～ 600 秒の範囲でメッセージの間隔を指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

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

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

アイドル状態での接続時間をデバイスが制限している場合でも、プロキシ、ファイアウォール、または NAT デバイスを介した SVC 接続を維持するように、キープアライブ メッセージの頻度（*seconds* で指定された）を調整できます。

頻度を調整することにより、Microsoft Outlook や Microsoft Internet Explorer などのソケット ベースのアプリケーションをユーザがアクティブに実行していないときに、SVC の切断や再接続が発生しないようにします。

例

次の例では、ユーザは、既存の Sales という名前のグループ ポリシーに対して、SVC がキープアライブ メッセージを 300 秒（5 分）の間隔で送信することをイネーブルにするようにセキュリティ アプライアンスを設定しています。

```
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対して SVC をイネーブルまたは必須にします。
svc dpd-interval	セキュリティ アプライアンスの Dead Peer Detection（DPD）をイネーブルにし、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定します。
svc keep-installer	リモート コンピュータへの SVC の永続的なインストールをイネーブルにします。
svc rekey	SVC セッションで SVC がキーの再生成を実行することをイネーブルにします。

svc keep-installer

リモート コンピュータへの SVC の永続的なインストレーションをイネーブルにするには、グループ ポリシー またはユーザ名の webvpn モードで **svc keep-installer** 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 keep-installer {**installed** | **none**}

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

シンタックスの説明

installed	リモート コンピュータに SVC が永続的にインストールされることを指定します。
none	アクティブな SVC 接続が終了した後で、リモート コンピュータから SVC をアンインストールするように指定します。

デフォルト

デフォルトでは、SVC の永続的なインストレーションはディセーブルになっています。SVC は SVC セッションの終了時にリモート コンピュータからアンインストールされます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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 ポリシーがリモート コンピュータへの SVC のインストールを維持するように設定しています。

```
hostname(config-group-policy)# svc keep-installer installed
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについて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 SVC をイネーブルまたは必須にします。
svc enable	セキュリティ アプライアンスに対して、SVC ファイルをフラッシュ メモリから RAM にダウンロードさせます。
svc image	セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定します。

svc rekey

SVC がキーの再生成を SVC セッションで実行することをイネーブルにするには、グループ ポリシーまたはユーザ名の webvpn 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 rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

シンタックスの説明

method ssl	SSL の再ネゴシエーションが SVC のキー再生成の間に行われることを指定します。
method new-tunnel	SVC が SVC のキー再生成の間に新しいトンネルを確立することを指定します。
time *minutes*	セッションの開始からキー再生成が行われるまでの分数を、4 ～ 10,080（1 週間）の範囲で指定します。
method none	SVC のキー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

次の表は、このコマンドを入力できるモードを示しています。

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

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

キー再生成の方式として SSL を設定することをお勧めします。

例

次の例では、既存の Sales という名前のグループ ポリシーに対して、キーの再生成の間に SSL が SVC と再ネゴシエーションするように設定し、キー再生成がセッションの開始後 30 分で発生するように設定しています。

```
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 SVC をイネーブルまたは必須にします。
svc dpd-interval	セキュリティ アプライアンスの Dead Peer Detection（DPD）をイネーブルにし、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定します。
svc keepalive	リモート コンピュータの SVC が、セキュリティ アプライアンスにキープアライブ メッセージを送信する頻度を指定します。
svc keep-installer	リモート コンピュータへの SVC の永続的なインストールをイネーブルにします。

switchport access vlan

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、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*

シンタックスの説明

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 は 1 ～ 1001 です。

デフォルト

デフォルトでは、スイッチ ポートはすべて VLAN 1 に割り当てられます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

透過ファイアウォール 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 ライセンスの場合はアクティブな VLAN を 2 つ、Security Plus ライセンスの場合は 3 つ設定できます。その内の 1 つはフェールオーバー用にする必要があります。

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 ライセンスの場合、アクティブな VLAN を 3 つまで、Security Plus ライセンスの場合は 20 まで設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定されている VLAN です。

switchport access vlan コマンドを使用して、各 VLAN に 1 つまたは複数の物理インターフェイスを割り当てることができます。デフォルトでは、そのインターフェイスの VLAN モードがアクセス 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）。インターフェイス上で複数の VLAN を通過させるトランク 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

次の例では、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 モードに入ります。
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	同じ VLAN 上でスイッチ ポートが他のスイッチ ポートと通信することを禁止して、セキュリティを大幅に強化します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport mode

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルの場合、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**}

シンタックスの説明

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 だけのトラフィックを通過させることができます。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。このモードでは、複数の VLAN のトラフィックを通過させることができます。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

デフォルトのモードは access です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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)	今までトランクは 1 つに制限されていましたが、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。複数の VLAN が通過するトランク ポートをスイッチ ポート上に作成する場合は、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場合、スイッチ ポートは「line protocol down」状態のままになり、トラフィックの転送には参加できません。トランク モードを使用できるのは、Security Plus ライセンスの場合のみです。

switchport vlan access コマンドは、モードをアクセス モードに設定しない限り有効になりません。**switchport trunk allowed vlan** コマンドは、モードをトランク モードに設定しない限り有効になりません。

例

次の例では、アクセス モードのスイッチ ポート（VLAN 100 を割り当て）、およびトランク モードのスイッチ ポート（VLAN 200 と 300 を割り当て）を設定しています。

```
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 モードに入ります。
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	同じ VLAN 上でスイッチ ポートが他のスイッチ ポートと通信することを禁止して、セキュリティを大幅に強化します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport protected

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、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同じ VLAN 上でスイッチ ポートが他の保護されたスイッチ ポートと通信することを禁止します。あるスイッチ ポートの安全性が確保されていない場合、この機能により VLAN 上の他のスイッチ ポートのセキュリティを向上させることができます。

switchport protected

no switchport protected

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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別の VLAN からアクセスされ、VLAN 内アクセスを許可する必要がなく、感染やその他のセキュリティ障害のときに各デバイスを隔離する場合は、スイッチ ポートが相互に通信することを禁止できます。たとえば、3 つの Web サーバをホスティングする DMZ が設定されている場合、**switchport protected** コマンドを各スイッチ ポートに適用する際には、各 Web サーバを隔離できます。内部と外部のネットワークはいずれも 3 つの Web サーバすべてと相互に通信できますが、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への通信とそのポートからの通信は、このコマンドによって制限されません。

例

次の例では、7 つのスイッチ ポートが設定されます。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、相互に保護されています。

```
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 モードに入ります。
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 allowed vlans

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、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 allowed vlans** 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。1 つまたは複数の 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*

no switchport trunk allowed vlans *vlan_range*

シンタックスの説明

vlan_range	トランク ポートに割り当て可能な 1 つまたは複数の VLAN を指定します。VLAN ID は 1 ～ 1001 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使用できますが、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。

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ません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 3 つ以上の VLAN を割り当てられるように修正されました。また、今までは 1 つのトランク ポートに限定されていましたが、複数のトランク ポートを設定できるようになりました。このコマンドでは、スペースの代わりにカンマを使用して VLAN ID を区切ることもできます。

使用上のガイドライン

複数の VLAN が通過するトランク ポートをスイッチ ポート上に作成する場合は、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。このスイッチ ポートについては、少なくとも 1 つの VLAN が割り当てられるまでは、トラフィックを通過させることができません。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場合、スイッチ ポートは「line protocol down」状態のままになり、トラフィックの転送には参加できません。トランク モードを使用できるのは、Security Plus ライセンスの場合のみです。

switchport trunk allowed vlan コマンドは、モードをトランク モードに設定しない限り有効になりません。

トランク ポートはタグのないパケットをサポートしません。ネイティブ VLAN はサポートされず、セキュリティ アプライアンスはこのコマンドで指定したタグを含んでいないパケットをすべてドロップします。

no switchport trunk allowed vlan コマンドを使用すると、すべての VLAN または VLAN のサブセットをトランクから削除できます。

（注） このコマンドは、バージョン 7.2(1) との下位互換性はなく、VLAN を区切るためのカンマは 7.2(1) では認識されません。ダウングレードした場合は、必ずスペースで VLAN を区切り、4 つ以上の VLAN を指定しないでください。

例

次の例では、アクセス モードのスイッチ ポートに VLAN 100 を割り当て、トランク モードのスイッチ ポートに VLAN 200、201、および 202 を割り当て、もう 1 つのトランク モードのスイッチ ポートに VLAN 300、301、および 305 を割り当てています。

```
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 200-202
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 300,301,305
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 モードに入ります。
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	同じ VLAN 上でスイッチ ポートが他のスイッチ ポートと通信することを禁止して、セキュリティを大幅に強化します。

syn-data

データを含んでいる 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**}

シンタックスの説明

allow	データを含んでいる SYN パケットを許可します。
drop	データを含んでいる 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、データを含んでいる SYN パケットは許可されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

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 モードに入ります。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、データを含んでいる SYN 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 パケットに含まれているデータを受け入れることが要件になっています。これは仕様の微妙かつあいまいな点であり、実装の中には、このパケットを適切に処理しないものもあります。不適切なエンドシステム実装を標的にする挿入攻撃に対して、脆弱にならないようにするには、データを含んでいる SYN パケットをドロップすることをお勧めします。

例

次の例は、データを含んでいる SYN パケットをすべての TCP フローでドロップする方法を示しています。

```
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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、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 トンネルを通してセキュリティ 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、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、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用します。グループ ポリシーおよびユーザごとの認可アクセス 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

この機能はデフォルトでイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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)(1)	このコマンドが、デフォルトでイネーブルになりました。また、バイパスされるのはインターフェイスのアクセス リストのみです。グループ ポリシーおよびユーザごとのアクセス リストは有効なままです。
7.1(1)	このコマンドが、**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 アプライアンスは 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を許可しています。したがって、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 リストに含め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 アドレスに対するインターフェイス 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するため、この機能により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もセキュリティ 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ごとの認可アクセス リストは、引き続きトラフィックに適用されます）。

インターフェイス アクセス リストをローカル IP アドレスに適用するには、**no sysopt connection permit-vpn** コマンドを入力します。アクセス リストの作成およびアクセス リストのインターフェイスへの適用については、**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ますが、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

次の例では、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 リストに従う必要があります。

```
hostname(config)# no sysopt connection permit-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドの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、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

TCP セグメントの最大サイズが設定した値を超えないようにし、指定したサイズよりも小さく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*]

シンタックスの説明

bytes	TCP セグメントの最大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 1,380 バイトです。*bytes* を 0 に設定することによって、この機能をディセーブルにできます。 ***minimum*** キーワードの場合、*bytes* は許容される最も小さい最大値を表します。
minimum	セグメントの最大サイズを上書きして、*bytes* 未満（48 ～ 65,535 バイト）にならないようにします。この機能は、デフォルトではディセーブルになっています（0 に設定されています）。

デフォルト

デフォルトの最大値は 1,380 バイトです。minimum 機能は、デフォルトではディセーブルになっています（0 に設定されています）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

ホストとサーバが接続を最初に確立するときは、ホストとサーバの両方でセグメントの最大サイズを設定できます。どちらかの最大サイズが **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 アプライアンスはその最大サイズを無効にして、設定した値を挿入します。どちらかの最大サイズが **sysopt connection tcpmss minimum** コマンドで設定した値よりも小さくなっている場合、セキュリティ アプライアンスはその最大サイズを無効にして、設定した「minimum」値を挿入します（minimum 値は、許容される最も小さい最大サイズです）。たとえば、最大サイズを 1,200 バイト、最小サイズを 400 バイトに設定した場合、ホストが最大サイズとして 1,300 バイトを要求しているときは、1,200 バイト（最大サイズ）を要求するようにセキュリティ アプライアンスがパケットを変更します。別のホストが最大値として 300 バイトを要求している場合、セキュリティ アプライアンスは 400 バイト（最小サイズ）を要求するようにパケットを変更します。

デフォルトの 1,380 バイトにしておくと、ヘッダー情報用の余裕ができるため、パケット全体のサイズが 1,500 バイトを超えることがなくなります。1,500 バイトは、イーサネットのデフォルト Maximum Transmission Unit（MTU; 最大伝送ユニット）です。次の計算式を参照してください。

1,380 データ + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1,500 バイト

ホストまたはサーバが最大セグメント サイズを要求しない場合、セキュリティ アプライアンスは、RFC 793 のデフォルト値である 536 バイトが有効であると想定します。

最大サイズを 1,380 バイトよりも大きい値に設定すると、MTU のサイズ（デフォルトは 1,500 バイト）によってはパケットがフラグメント化される可能性があります。フラグメントが大量に発生すると、セキュリティ アプライアンスが Frag Guard 機能を使用している場合にパフォーマンスに影響する可能性があります。最小サイズを設定しておくと、TCP サーバが小さな TCP データ パケットをクライアントに大量に送信して、サーバとネットワークのパフォーマンスに影響を与えることを防止できます。

（注）　この機能を普通に使用する場合にはお勧めしませんが、syslog IPFRAG メッセージ 209001 および 209002 が発生する場合は、*bytes* 値を大きくできます。

例

次の例では、最大サイズを 1,200 バイト、最小サイズを 400 バイトに設定しています。

```
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** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドの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

最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が少なくとも 15 秒の短縮 TIME_WAIT 状態を保持するようにするには、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は、この機能を使用することをお勧めします。

sysopt connection timewait

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

この機能は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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、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 アプライアンスは、標準クローズ シーケンスと呼ばれる一般的なクロージング シーケンスに基づいて、高接続率を保つことができます。ただし、一方のエンドがクローズし、もう一方のエンドは確認応答してからクロージング シーケンスを開始する標準クローズ シーケンスとは対照的に、同時クローズでは、トランザクションの両エンドがクロージング 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、即時解放により、接続の 1 つのサイドで CLOSING 状態が保持されます。CLOSING 状態の多くのソケットがある場合は、エンド ホストのパフォーマンスが低下することがあります。たとえば、一部の WinSock メインフレーム クライアントは、このような動作を示し、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確認されています。**sysopt connection timewait** コマンドを使用すると、同時クローズ ダウン シーケンスを完了するためのウィンドウが作成されます。

例

次の例では、timewait（一時停止）機能をイネーブルにしています。

```
hostname(config)# sysopt connection timewait
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドの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、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場合に、DNS の A レコード アドレスを変更する DNS 検査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 だけを実行して、DNS パケットの変更が不要な場合には、DNS アプリケーション検査をディセーブルにすることをお勧めします。

sysopt nodnsalias {***inbound*** | ***outbound***}

no sysopt nodnsalias {***inbound*** | ***outbound***}

シンタックスの説明

inbound	セキュリティの低いインターフェイスから、**alias** コマンドで指定したセキュリティの高いインターフェイスに向かうパケットの DNS レコード変更をディセーブルにします。
outbound	**alias** コマンドで指定した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に向かうパケットの DNS レコード変更をディセーブルにします。

デフォルト

この機能は、デフォルトではディセーブルになっています。つまり、DNS レコードのアドレス変更がイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

alias コマンドは、NAT、および DNS の A レコードのアドレス変更を実行します。DNS レコードの変更は、特定の状況下ではディセーブルにした方がよい場合もあります。

例

次の例では、着信パケットについて DNS アドレスの変更をディセーブルにしています。

```
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、変換に対応するように DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt noproxyarp	インターフェイス上でのプロキシ ARP をディセーブルにします。

sysopt noproxyarp

NAT グローバル アドレスに対するインターフェイス上でのプロキシ 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。グローバル アドレスに対するプロキシ 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*

シンタックスの説明

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

デフォルトでは、グローバル アドレスに対するプロキシ ARP はイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

まれに、グローバル アドレスに対するプロキシ ARP をディセーブルにした方がよい場合もあります。

ホストが IP トラフィックを同じイーサネット ネットワーク上の別のデバイスに送信するとき、ホストはデバイスの MAC アドレスを知っている必要があります。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、「この IP アドレスは誰なのか」という ARP 要求を送信します。当該の IP アドレスを所有しているデバイスは、「その IP アドレスを所有している。これが私の MAC アドレスだ」という応答を返します。

プロキシ ARP は、デバイスが当該の IP アドレスを所有していない場合でも、デバイスが自身の MAC アドレスで ARP 要求に応答する動作です。NAT を設定して、セキュリティ アプライアンス 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 アプライアンスはプロキシ ARP を使用します。トラフィックがホストに到達する唯一の方法は、セキュリティ アプライアンスがプロキシ ARP を使用して、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

次の例では、内部インターフェイス上でのプロキシ ARP をディセーブルにしています。

```
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、変換に対応するように DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドの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 の 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に含まれている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 サーバとの互換性を維持するには、このキーを無視する必要があります。

sysopt radius ignore-secret

no sysopt radius ignore-secret

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

この機能は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

Livingston Version 1.16 など、一部の RADIUS サーバでは、アカウンティング確認応答の認証ハッシュ内にキーが含まれていないという使用上の注意点があります。このような場合、セキュリティ アプライアンスがアカウンティング要求を継続的に再送信することがあります。**sysopt radius ignore-secret** コマンドは、アカウンティング確認応答の認証キーを無視して、再送信の問題を回避するために使用します。ここで説明しているキーとは、**aaa-server host** コマンドで設定するキーです。

例

次の例では、アカウンティング応答に含まれている認証キーを無視しています。

```
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** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。