CHAPTER 15

# packet-tracer コマンド～ ping コマンド

## packet-tracer

packet-tracer コマンドを特権 EXEC モードで使用すると、ファイアウォールの現在の設定に対して 5 ～ 6 タプルのパケットを生成することができます。ここでは、わかりやすいように、ICMP、CP/UDP/SCTP、および IP の各パケットのモデリング別に packet-tracer の構文を示します。

**packet-tracer input** *ifc_name* [**vlan-id** *vlan_id*] **icmp** [**inline-tag** *tag*] {*sip* | **user** *username* | **security-group {name** *name* | **tag** *tag*} | **fqdn** *fqdn_string*} *icmp_code* [*icmp_id*] [*dmac*] {*dst_ip* | **security-group {name** *name* | **tag** *tag*} | **fqdn** *fqdn_string*} [**detailed**] [**xml**]

**packet-tracer input** *ifc_name* [**vlan-id** *vlan_id*] **rawip** [**inline-tag** *tag*] {*sip* | **user** *username* | **security-group {name** *name* | **tag** *tag*} | **fqdn** *fqdn_string*} *protocol* [*dmac*] {*dst_ip* | **security-group {name** *name* | **tag** *tag*} | **fqdn** *fqdn_string*} [**detailed**] [**xml**]

**packet-tracer input** *ifc_name* **[vlan-id** ***vlan_id***] **{tcp | udp | sctp} [inline-tag** ***tag***] **{***sip* | **user** *username* | **security-group {name** *name* | **tag** *tag*} | **fqdn** *fqdn_string*} *src_port* [*dmac*] **{***dst_ip* | **security-group {name** *name* | **tag** *tag*} | **fqdn** *fqdn_string*} *dst_port* **[{vxlan-inner** *vxlan_inner_tag* **icmp** *inner_src_ip inner_icmp_type inner_icmp_code* [*inner_icmp_id*] *inner_dst_ip inner_src_mac inner_dst_mac*} | **{vxlan-inner** *vxlan_inner_tag* **rawip** *inner_src_ip inner_protocol inner_dst_ip inner_src_mac inner_dst_mac*} | **{vxlan-inner** *vxlan_inner_tag* **{tcp | udp | sctp}** *inner_src_ip inner_src_port inner_dst_ip inner_dst_port inner_src_mac inner_dst_mac*}] **[detailed] [xml]**

**構文の説明**

| | |
|---|---|
| **detailed** | (オプション)トレース結果の詳細な情報を表示します。 |
| *dmac* | 宛先 MAC アドレスを指定します。出力インターフェイスの選択肢を表示することで交換されたパケットの寿命に関する全体像を提供するとともに、宛先 MAC アドレスが不明であったことによるパケット ドロップも提供します。 |
| *dst_ip* | パケット トレースの宛先アドレス(IPv4 または IPv6)を指定します。 |
| *dst_port* | TCP/UDP/SCTP パケット トレースの宛先ポートを指定します。 |
| **fqdn** *fqdn_string* | ホストの完全修飾ドメイン名を指定します。送信元と宛先のどちらの IP アドレスにも使用できます。IPv4 の FQDN のみがサポートされます。 |
| **icmp** | 使用するプロトコルとして ICMP を指定します。 |
| *icmp_code* | ICMP パケット トレースの ICMP コードを指定します。 |

| | |
|---|---|
| *icmp_id* | (任意)ICMP パケット トレースの ICMP ID を指定します。 |
| *inner_dst_ip* | 内部パケットの宛先アドレス(IPv4 または IPv6)を指定します。 |
| *inner_dst_mac* | 内部パケットの宛先 MAC アドレスを指定します。 |
| *inner_dst_port* | 内部パケットの宛先ポートを指定します。 |
| *inner_icmp_code* | 内部パケットの ICMP タイプ コードを指定します。 |
| *inner_icmp_type* | 内部パケットの識別済み ICMP メッセージを指定します。 |
| *inner_protocol* | 内部パケットのプロトコル番号を指定します。 |
| *inner_src_mac* | 内部パケットのスプール MAC アドレスを指定します。 |
| *inner_src_ip* | 内部パケットの送信元アドレス(IPv4 または IPv6)を指定します。 |
| **input** *ifc_name* | パケットの入力インターフェイスを指定します。 |
| **inline-tag** *tag* | レイヤ 2 CMD ヘッダーに埋め込まれているセキュリティ グループ タグの値を指定します。有効な値の範囲は 0 ～ 65533 です。 |
| *protocol* | raw IP パケット トレーシングのプロトコル番号(0 ～ 255)を指定します。 |
| **rawip** | 使用するプロトコルとして raw IP を指定します。 |
| **sctp** | 使用するプロトコルとして SCTP を指定します。 |
| **security-group** {**name** *name* \| **tag** *tag* } | TrustSec の IP-SGT ルックアップに基づいて送信元と宛先のセキュリティ グループを指定します。セキュリティ グループの名前またはタグ番号を指定できます。 |
| *src_port* | TCP/UDP/SCTP パケット トレースの送信元ポートを指定します。 |
| **tcp** | 使用するプロトコルとして TCP を指定します。 |
| *type* | ICMP パケット トレースの ICMP タイプを指定します。 |
| **udp** | 使用するプロトコルとして UDP を指定します。 |
| **user** *username* | 送信元 IP アドレスとしてユーザを指定する場合に *domain\user* の形式でユーザ アイデンティティを指定します。ユーザに対して最後にマッピングされたアドレス(複数ある場合)がトレースに使用されます。 |
| **vlan-id** *vlan_id* | (オプション)フローの VLAN アイデンティティを指定します。有効範囲は 1 ～ 4096 です。 |
| **vxlan-inner** *vxlan_inner_tag* | VXLAN カプセル化を使用して内部パケットを指定します。 |
| **xml** | (オプション)トレース結果を XML 形式で表示します。 |

**コマンド デフォルト**

このコマンドには、デフォルト設定がありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが追加されました。 |
| 8.4(2) | キーワードと引数のペアが 2 組追加されました（**user** *username* と **fqdn** *fqdn_string*.）。いくつかのキーワードの名前と定義が変更されました。IPv6 送信元アドレスのサポートが追加されました。 |
| 9.0(1) | ユーザ アイデンティティのサポートが追加されました。IPv4 の完全修飾ドメイン名（FQDN）のみがサポートされます。 |
| 9.3(1) | キーワードと引数のペア **inline-tag** *tag* が追加され、レイヤ 2 CMD ヘッダーに埋め込まれているセキュリティ グループ タグの値がサポートされるようになりました。 |
| 9.4(1) | キーワードと引数のペアが 2 つ追加されました（**vlan-id** *vlan_id* と **vxlan-inner** *vxlan_inner_tag*）。 |
| 9.5(2) | **sctp** キーワードが追加されました。 |
| 9.7(1) | トランスペアレント ファイアウォール モードのサポート。宛先 MAC アドレスに新しいトレース モジュールが追加されました。 |
| 9.9.(1) | 永続的なトレースをクラスタリングするためのサポートが導入されました。この機能によって、クラスタ ユニットでパケットを追跡できます。新しいオプションの *persist*、*bypass-checks*、*decrypted*、*transmit*、*id*、および *origin* が追加されました。 |

## 使用上のガイドライン

**Capture** コマンドによるパケットのキャプチャに加えて、ASA を介してパケットの寿命をトレースして、想定どおりに動作しているかどうかを確認できます。**packet-tracer** コマンドを使用すると、次の操作を実行できます。

- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用可能なすべてのルール、およびルールが追加される原因となった CLI 行を表示する。
- データ パスのパケット変更をタイムラインで表示する。
- データ パスにトレーサ パケットを挿入する。
- ユーザ アイデンティティおよび FQDN に基づいて IPv4 アドレスまたは IPv6 アドレスを検索する。
- クラスタ ノード間でパケットをデバッグする。

**packet-tracer** コマンドは、パケットに関する詳細情報と、ASA によるパケットの処理方法を提供します。ファイアウォール管理者は、packet-tracer を使用して、セキュリティ アプライアンスに仮想パケットを送信し、入口から出口へのフローを追跡できます。その途中で、フローおよびルート ルックアップ、ACL、プロトコル インスペクション、および NAT に対してパケットが評価されます。ユーティリティの能力は、送信元および宛先のアドレスと、プロトコルおよびポート情報を指定して実際のトラフィックをシミュレートする機能によってもたらされます。

オプションの **vlan-id** キーワードを使用すると、パケット トレーサがペアレント インターフェイスに入ることができ、その後に VLAN アイデンティティと一致するサブインターフェイスにリダイレクトされます。VLAN アイデンティティは、サブインターフェイス以外だけに使用可能なオプション エントリです。管理インターフェイスは例外です。ペアレント管理専用インターフェイスが持つことができるのは管理専用サブインターフェイスだけです。

宛先 MAC アドレスのルックアップを使用できます。

トランスペアレント ファイアウォール モードでは、入力インターフェイスが VTEP の場合に、VLAN に値を入力すると宛先 MAC アドレスはオプションで有効になります。一方、ブリッジ グループ メンバー インターフェイスでは、宛先 MAC アドレスは必須フィールドですが、**vlan-id** キーワードを入力した場合はオプションになります。

ルーテッド ファイアウォール モードでは、入力インターフェイスがブリッジ グループ メンバー インターフェイスの場合、**vlan-id** と *dmac* 引数はオプションです。

次の表に、トランスペアレント ファイアウォール モードとルーテッド ファイアウォール モードでのそれぞれの VLAN アイデンティティと宛先 MAC アドレスのインターフェイス依存型の動作に関する詳しい情報を示します。

**トランスペアレント ファイアウォール モード**

| インターフェイス | VLAN | 宛先 MAC アドレス |
|---|---|---|
| **管理** | イネーブル（オプション） | 無効 |
| **VTEP** | イネーブル（オプション） | ディセーブルユーザが VLAN に値を入力すると、宛先 MAC アドレスはイネーブルになりますが、これはオプションです。 |
| **ブリッジ仮想インターフェイス（BVI）** | イネーブル（オプション） | イネーブル（必須）ユーザが VLAN に値を入力した場合、宛先 MAC アドレスはオプションです。 |

**ルーテッド ファイアウォール モード**

| インターフェイス | VLAN | 宛先 MAC アドレス |
|---|---|---|
| **管理** | イネーブル（オプション） | 無効 |
| **ルーテッド インターフェイス** | イネーブル（オプション） | 無効 |
| **ブリッジ グループ メンバー** | イネーブル（オプション） | イネーブル（オプション） |

入力インターフェイスを使用して **packet-tracer** コマンドを実行しているときにパケットがドロップされない場合、そのパケットは UN-NAT、ACL、NAT、IP-OPTIONS、FLOW-CREATION のようなさまざまなフェーズを通過します。その結果、「**ALLOW**」というメッセージが表示されます。

ファイアウォール設定によってライブ トラフィックがドロップされる可能性があるシナリオでは、シミュレーションされたトレーサ パケットもドロップされます。場合によっては、ドロップの特定の理由が表示されることがあります。たとえば、ヘッダーの検証が無効なためパケットがドロップされた場合、「packet dropped due to bad ip header (reason)」というメッセージが表示されます。宛先 MAC アドレスが不明な場合は、スイッチング シーケンスでパケットがドロップされます。これにより宛先 MAC アドレスを検索するように ASA が起動されます。MAC アドレスが見つかった場合は、packet-tracer を再度実行することができ、宛先 L2 ルックアップに成功します。

パケット トレーサでの VXLAN サポートにより、内部パケットのレイヤ 2 送信元と宛先 MAC アドレス、レイヤ 3 送信元と宛先 IP アドレス、レイヤ 4 プロトコル、レイヤ 4 送信元と宛先ポート番号、仮想ネットワーク インターフェイス（VNI）番号を指定することができます。TCP、SCTP、UDP、raw IP、および ICMP のみが内部パケットでサポートされます。

ドメイン/ユーザの形式を使用して送信元のユーザ アイデンティティを指定できます。ASA では、そのユーザの IP アドレスを検索し、該当する IP アドレスをパケット トレースのテストで使用します。ユーザが複数の IP アドレスにマッピングされている場合、最後にログインした IP アドレスが使用され、IP アドレスとユーザのマッピングがほかにもあることを示す出力が表示されます。このコマンドの送信元の部分でユーザ アイデンティティを指定した場合、ASA では、ユーザが入力した宛先アドレスのタイプに基づいて IPv4 または IPv6 のいずれかのアドレスを検索します。

セキュリティ グループ名またはセキュリティ グループ タグを送信元として指定できます。ASA では、そのセキュリティ グループ名またはセキュリティ グループ タグに基づいて IP アドレスを検索し、該当する IP アドレスをパケット トレースのテストで使用します。セキュリティ グループ タグまたはセキュリティ グループ名が複数の IP アドレスにマッピングされている場合、それらのいずれかの IP アドレスが使用され、IP アドレスとセキュリティ グループ タグのマッピングがほかにもあることを示す出力が表示されます。

また、送信元と宛先アドレスの両方に FQDN を指定できます。ASA では、DNS ルックアップを実行し、パケットの構造で最初に返された IP アドレスを取得します。

L3 からブリッジ仮想インターフェイス、ブリッジ仮想インターフェイスからブリッジ仮想インターフェイスなど、宛先 IP が ASA 上の BVI インターフェイスを通じたネクスト ホップの場合のトラフィック シナリオでは、パケット トレーサはダブル ルートルックアップを実行します。また、フローは作成されません。

ARP と MAC アドレス テーブル エントリをクリアすることで、パケット トレーサは常にダブルルートルックアップを実行し、宛先 MAC アドレスが解決されてデータベースに保存されます。しかし、これはその他のトラフィック シナリオには当てはまりません。L3 インターフェイスである場合は、宛先 MAC アドレスは解決されずにデータベースに保存されます。BVI インターフェイスは *nameif* で設定され、L3 プロパティがあるため、DMAC ルックアップを実行してはなりません。

MAC アドレスと ARP エントリがない場合の初回の試行にだけ、この動作が見られます。DMAC にエントリがあれば、パケット トレーサの出力は予期どおりになります。フローが作成されます。

永続的トレースによって、パケットがクラスタ ユニット間を通過するときにトレースできます。クラスタ ユニット間で追跡するパケットは永続化オプションを使用して送信する必要があります。各パケットの永続的なトレースのために、packet-id とホップ カウントが用意されており、送信されたパケットの起点とクラスタ ノードを通過するパケットのホップのフェーズを判断できます。packet-id は、<*パケットが発信されたデバイスのノード名*> と増分値の組み合わせです。packet-id は、ノードで初めて受信する新しいパケットごとに一意です。ホップ カウントは、パケットがあるクラスタ メンバーから別のクラスタ メンバーに移動するたびに読み込まれます。たとえば、クラスタリングにおいてパケットは、外部の負荷分散番号付きリストに基づいてメンバーに到着します。Host-1 は、Host-2 にパケットを送信します。送信されたパケットは、Host-2 に送信される前に、クラスタ ノード間でリダイレクトされます。メタデータの出力で、`Tracer origin-id B:7 hop 0`、`Tracer origin-id B:7 hop 1`、および `Tracer origin-id B:7 hop 2` がそれぞれ表示されます。B は、パケットの発信元であるクラスタ ノードの名前です。7 は増分値で、クラスタ ノードから発信された 7 番目のパケットを表します。この値は、ノードから新しいパケットが発信されるたびに増やされます。"B" と "7"の組み合わせによって、パケットを特定する一意の ID が形成されます。クラスタ ユニットのローカル名は、このユニットを通過するすべてのパケットで同じです。各パケットは、グローバル バッファが unique-id とホップ カウントを使用するときに区別されます。パケットがトレースされると、永続的トレースが各ノードで使用可能になります。これは、メモリを解放するために手動で破棄するまで継続します。あるコンテキストで有効な永続的トレースは、コンテキストごとのバッファに格納されます。一連のトレースの中で特定のトレースを検索するには、origin-owner-ID（<origin-owner> <id> の 2 つの値）を使用します。

この場合、ASA から出力されるパケットをシミュレートすることができます。packet-tracer を介して transmit オプションを使用することにより、ネットワークでパケットを送信できます。デフォルトでは、packet-tracer はパケットを転送する前に廃棄します。パケットが出力されると、フロー テーブルでフローが生成されます。

packet-tracer で bypass-checks オプションを使用することにより、ACL、VPN フィルタ、uRPF、および IPsec スプーフィング チェックをバイパスできます。これは入力と出力条件の両方に適用され、シミュレートされた IPSec パケットはドロップされません

VPN トンネル内で復号化されたパケットを送信できます。VPN トンネルは汎用的で IPSec と TLS の両方に適用できます。VPN トンネル経由で送信されるパケットをシミュレートすることもできます。シミュレートされた '復号化' パケットは、既存の VPN トンネルに対応し、関連するトンネルポリシーが適用されます。

## 例

次に、HTTP ポート 201.1.1.1 から 202.1.1.1 への TCP パケットをトレースする例を示します。

```
ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a
detailed

Result:
Action: drop
Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed

ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a
detailed

Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC Address Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC address lookup resulted in egress ifc outside
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fdbe83542f0, priority=1, domain=permit, deny=false
hits=7313, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fdbd94026a0, priority=12, domain=permit, deny=false
hits=8, user_data=0x7fdbf07cbd00, cs_id=0x0, use_real_addr,
flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=10, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=6x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fdbe8363790, priority=0, domain=inspect-ip-options, deny=true
hits=212, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 6
Type: NAT Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
```

```
hits=12, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=6x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x7fdbd93dfc10, priority=0, domain=inspect-ip-options, deny=true
hits=110, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 221, packet dispatched to next module
Module information for forward flow …
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow …
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
126# command example
ciscoasa(config)# command example
resulting screen display here
<Text omitted.>
```

次に、HTTP ポート 10.100.10.10 から 10.100.11.11 への TCP パケットをトレースする例を示します。暗黙の拒否アクセス ルールによってパケットがドロップされることを示す結果が表示されます。

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
```

```
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc outside

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

次に、ユーザ CISCO\abc による内部ホスト 10.0.0.2 から外部ホスト 20.0.0.2 へのパケットをトレースする例を示します。

```
ciscoasa# packet-tracer input inside icmp user CISCO\abc 0 0 1 20.0.0.2

Source: CISCO\abc 10.0.0.2

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 20.0.0. 255.255.255.0 outside
...
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interfce: outside
output-status: up
output-line-status: up
Action: allow
```

次に、ユーザ CISCO\abc による内部ホスト 20.0.0.2 からのパケットをトレースし、トレース結果を XML 形式で表示する例を示します。

```
<Source>
<user>CISCO\abc</user>
<user-ip>10.0.0.2</user-ip>
<more-ip>1</more-ip>
</Source>

<Phase>
<id>1</id>
<type>ROUTE-LOOKUP</type>
<subtype>input</subtype>
<result>ALLOW</result>
<config>
</config>
<extra>
in 20.0.0.0 255.255.255.0 outside
```

```
</extra>
</Phase>
```

次に、内部ホスト xyz.example.com から外部ホスト abc.example.com へのパケットをトレースする例を示します。

```
ciscoasa# packet-tracer input inside tcp fqdn xyz.example.com 1000 fqdn abc.example.com 23
Mapping FQDN xyz.example.com to IP address 10.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)

Mapping FQDN abc.example.com to IP address 20.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

次に、**packet-tracer** コマンドの出力例を示します。この出力から、セキュリティ グループ タグと IP アドレスの対応付けがわかります。

```
ciscoasa# packet-tracer input inside tcp security-group name alpha 30 security-group tag
31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

次に、レイヤ 2 SGT インポジションを表示する **packet-tracer** コマンドの出力の例を示します。

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 10.1.1.2 30 192.168.1.2 300
```

次の例では、UDP/TCP および ICMP の内部パケットに対する VXLAN のサポートについて概要を示します。

```
packet-tracer in inside udp 30.0.0.2 12345 30.0.0.100 vxlan vxlan-inner 1234 1.1.1.1 11111
2.2.2.2 22222 aaaa.bbbb.cccc aaaa.bbbb.dddd detailed

Outer packet: UDP from 30.0.0.2 to 30.0.0.100 (vtep/nve source-interface IP) with default
vxlan destination port.
Inner packet: VXLAN in-tag 1234, UDP from 1.1.1.1/11111 to 2.2.2.2/22222 with smac
aaaa.bbbb.cccc and dmac aaaa.bbbb.dddd
```

次に、クラスタ ユニット間で渡される永続的トレースの出力の例を示します。

```
ciscoasa# cluster exec show packet-tracer
B(LOCAL):**********************************************************
tracer 10/8 (allocate/freed), handle 10/8 (allocated/freed), error 0
======= Tracer origin-id B:7, hop 0 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)

<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
```

```
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) am asking director (0).

Phase: 5
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To A(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10

======= Tracer origin-id B:7, hop 2 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)

<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>

Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From A(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10

<Snipping phase 2-4: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>

Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) have been elected owner by (0).

<Snipping phase 6-16: ACCESS-LIST, NAT, IP-OPTIONS, INSPECT, INSPECT, FLOW-CREATION,
ACCESS-LIST, NAT, IP-OPTIONS, ROUTE-LOOKUP, ADJACENCY-LOOKUP>

A:**********************************************************************
tracer 6/5 (allocate/freed), handle 6/5 (allocated/freed), error 0
======= Tracer origin-id B:7, hop 1 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)

Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From B(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10

<Snipping phase 2-7: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP, ACCESS-LIST, NAT, IP-OPTIONS>

Phase: 8
Type: CLUSTER-EVENT
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (0) am director, not creating dir flow for ICMP pkt recvd by (1).

Phase: 9
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To B(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
ciscoasa#
```

次に、origin と id のオプションを使用してクラスタ ノードからパケットがトレースされるときの出力の例を示します。

```
cluster2-asa5585a# cluster exec show packet-tracer | i origin-id
b(LOCAL):**************************************************************
======= Tracer origin-id b:2, hop 0 =======
======= Tracer origin-id b:2, hop 2 =======

a:**************************************************************
======= Tracer origin-id a:17, hop 0 =======
======= Tracer origin-id b:2, hop 1 =======
======= Tracer origin-id b:2, hop 3 =======
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer ori
cluster2-asa5585a# cluster exec show packet-tracer origin b id 2
b(LOCAL):**************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
======= Tracer origin-id b:2, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity

Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) am asking director (0).
```

```
Phase: 4
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10

Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

======= Tracer origin-id b:2, hop 2 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)

Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From a(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) have been elected owner by (0).

Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
```

```
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: FULL
I (1) am redirecting to (0) due to matching action (1).
```

```
Phase: 15
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10

Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

a:**********************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
======= Tracer origin-id b:2, hop 1 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)

Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am director, found static rule to classify owner as (253).

Phase: 7
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To b(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10

Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

======= Tracer origin-id b:2, hop 3 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)

Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) have been elected owner by (0).

Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
```

```
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 15
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 17
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 18
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 70, packet dispatched to next module

Phase: 19
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc identity

Phase: 20
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address 0000.0000.0000 hits 1730 reference 6

Phase: 21
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
ifc selected is not same as preferred ifc
Doing route lookup again on ifc outside2

Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

cluster2-asa5585a#
cluster2-asa5585a#
```

```
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer origin a
b(LOCAL):**********************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0


a:**********************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
======= Tracer origin-id a:17, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity

Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
```

```
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc identity

Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address 0000.0000.0000 hits 1577 reference 6

Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer id 17
b(LOCAL):****************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0

a:****************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
======= Tracer origin-id a:17, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity

Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 4
Type: NAT
Subtype: per-session
```

```
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
```

```
Config:
Additional Information:

Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module

Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc identity

Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address 0000.0000.0000 hits 1577 reference 6

Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

cluster2-asa5585a#
```

次の例では、クラスタ ノードからの永続的トレースをクリアする概要を示します。

```
ciscoasa# cluster exec clear packet-tracer
```

IPSec トンネルで復号化されたパケットを送信する場合は、いくつかの条件があります。IPSec トンネルがネゴシエートされていない場合、エラー メッセージが表示されます。次に、IPSec トンネルがネゴシエートされると、パケットが通過します。

次の例では、復号化されたパケットを送信するために IPSec トンネルがネゴシエート**されない**場合の概要を示します。

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
decrypted

 ****************************************************************
 WARNING: An existing decryption SA was not found. Please confirm the
 IPsec Phase 2 SA or Anyconnect Tunnel is established.
 ****************************************************************

 Phase: 1
 Type: ACCESS-LIST
 Subtype:
 Result: ALLOW
 Config:
 Implicit Rule
 Additional Information:
 MAC Access list

 Phase: 2
 Type: ROUTE-LOOKUP
 Subtype: Resolve Egress Interface
 Result: ALLOW
 Config:
 Additional Information:
 found next-hop 214.1.1.9 using egress ifc  outside2

 Phase: 3
 Type: CLUSTER-EVENT
 Subtype:
 Result: ALLOW
 Config:
 Additional Information:
 Input interface: 'outside'
 Flow type: NO FLOW
 I (0) got initial, attempting ownership.

 Phase: 4
 Type: CLUSTER-EVENT
 Subtype:
 Result: ALLOW
 Config:
 Additional Information:
 Input interface: 'outside'
 Flow type: NO FLOW
 I (0) am becoming owner

 Phase: 5
 Type: ACCESS-LIST
 Subtype: log
 Result: ALLOW
 Config:
 access-group ALLOW global
 access-list ALLOW extended permit ip any any
 Additional Information:

 Phase: 6
 Type: NAT
 Subtype: per-session
 Result: ALLOW
 Config:
 Additional Information:

 Phase: 7
 Type: IP-OPTIONS
```

```
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect ftp
service-policy global_policy global
Additional Information:

Phase: 9
Type: VPN
Subtype: ipsec-tunnel-flow
Result: DROP
Config:
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule

cluster2-asa5585a(config)#
```

次の例では、復号化されたパケットを送信するために IPSec トンネルがネゴシエートされた場合の概要を示します。

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21 decrypted

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.

Phase: 3
Type: CLUSTER-EVENT
```

```
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
```

```
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 19
```

```
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 20
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 21
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1099, packet dispatched to next module

Phase: 22
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 23
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 24
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 25
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1100, packet dispatched to next module

Phase: 26
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
```

```
  Result: ALLOW
  Config:
  Additional Information:
  adjacency Active
  next-hop mac address 4403.a74a.9a32 hits 99 reference 2

  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: allow
```

次の例では、送信オプションを使用して、シミュレートされたパケットの送信を許可し、発信インターフェイスで同じパケットをキャプチャします。

```
cluster2-asa5585a(config)# packet-tracer input outside icmp 211.1.1.10 8 0 213.1.1.10
transmit

  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list

  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list

  Phase: 3
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2

  Phase: 4
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) am becoming owner

  Phase: 5
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
  access-list ALLOW extended permit ip any any
```

```
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
  New flow created with id 6449, packet dispatched to next module

  Phase: 15
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
  access-list ALLOW extended permit ip any any
  Additional Information:

  Phase: 16
  Type: NAT
  Subtype: per-session
  Result: ALLOW
  Config:
  Additional Information:

  Phase: 17
  Type: IP-OPTIONS
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:

  Phase: 18
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2

  Phase: 19
  Type: ADJACENCY-LOOKUP
  Subtype: next-hop and adjacency
  Result: ALLOW
  Config:
  Additional Information:
  adjacency Active
  next-hop mac address 4403.a74a.9a32 hits 15 reference 1

  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: allow

  cluster2-asa5585a(config)#
```

次の例では、発信インターフェイスでキャプチャされる ICMP パケットの概要を示します。

```
cluster2-asa5585a(config)# cluster exec show capture test | i icmp
  a(LOCAL):*******************************************************
    14: 02:18:16.717736       802.1Q vlan#212 P0 211.1.1.10 > 213.1.1.10: icmp: echo
request

  cluster2-asa5585a(config)#
```

packet-tracer の bypass-checks オプションの例については、以下のフェーズで概要を示します。各シナリオでは、特定の例が想定されています。

- スポークとハブ間に IPSec トンネルが作成されない場合。
- 2 つのボックス間で IPSec トンネルをネゴシエートする必要があり、最初のパケットがトンネルの確立をトリガーします。
- IPSec ネゴシエーションが完了し、トンネルが生成されます。
- トンネルが起動すると、発信されるパケットはトンネルを介して送信されます。パケット パスで使用できるセキュリティ チェック（ACL、VPN フィルタリング..）がバイパスまたはスキップされます。

IPSec トンネルは作成されません。

```
cluster2-asa5585a(config)# sh crypto ipsec sa

  There are no ipsec sas
  cluster2-asa5585a(config)#
```

トンネル ネゴシエーション プロセスが開始されます。

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
bypass-checks

  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list

  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list

  Phase: 3
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2

  Phase: 4
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.
```

```
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner

Phase: 6
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:

Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
```

```
  service-policy global_policy global
  Additional Information:

  Phase: 12
  Type: VPN
  Subtype: ipsec-tunnel-flow
  Result: ALLOW
  Config:
  Additional Information:

  Phase: 13
  Type: VPN
  Subtype: encrypt
  Result: DROP
  Config:
  Additional Information:

  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: drop
  Drop-reason: (acl-drop) Flow is denied by configured rule

  cluster2-asa5585a(config)#
```

IPSec トンネルがネゴシエートされると、トンネルが生成されます。

```
cluster2-asa5585a#

  cluster2-asa5585a(config)# sh crypto ipsec sa
  interface: outside2
      Crypto map tag: crypto-map-peer4, seq num: 1, local addr: 214.1.1.10

        access-list toPeer4 extended permit ip host 211.1.1.1 host 213.1.1.2
        local ident (addr/mask/prot/port): (211.1.1.1/255.255.255.255/0/0)
        remote ident (addr/mask/prot/port): (213.1.1.2/255.255.255.255/0/0)
        current_peer: 214.1.1.9


        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
        #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
        #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
        #TFC rcvd: 0, #TFC sent: 0
        #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
        #send errors: 0, #recv errors: 0

        local crypto endpt.: 214.1.1.10/500, remote crypto endpt.: 214.1.1.9/500
        path mtu 1500, ipsec overhead 74(44), media mtu 1500
        PMTU time remaining (sec): 0, DF policy: copy-df
        ICMP error validation: disabled, TFC packets: disabled
        current outbound spi: A642726D
        current inbound spi : CF1E8F90

      inbound esp sas:
        spi: 0xCF1E8F90 (3474886544)
           SA State: active
```

```
            transform: esp-aes-256 esp-sha-hmac no compression
            in use settings ={L2L, Tunnel, IKEv2, }
            slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
            sa timing: remaining key lifetime (kB/sec): (4285440/28744)
            IV size: 16 bytes
            replay detection support: Y
            Anti replay bitmap:
             0x00000000 0x00000001
        outbound esp sas:
          spi: 0xA642726D (2789372525)
            SA State: active
            transform: esp-aes-256 esp-sha-hmac no compression
            in use settings ={L2L, Tunnel, IKEv2, }
            slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
            sa timing: remaining key lifetime (kB/sec): (4239360/28744)
            IV size: 16 bytes
            replay detection support: Y
            Anti replay bitmap:
             0x00000000 0x00000001

  cluster2-asa5585a(config)#
```

トンネルが生成されるとパケットが通過できるようになり、bypass-checks オプションが適用されるため、セキュリティ チェックがスキップされます。

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
bypass-checks

  Phase: 1
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2

  Phase: 2
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.

  Phase: 3
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) am becoming owner

  Phase: 4
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
  access-list ALLOW extended permit ip any any
```

```
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:

Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 12
```

```
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 19
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 20
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 21
Type: FLOW-CREATION
```

```
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1099, packet dispatched to next module

Phase: 22
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 23
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 24
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 25
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1100, packet dispatched to next module

Phase: 26
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address 4403.a74a.9a32 hits 99 reference 2

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: allow
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **capture** | トレース パケットを含めて、パケット情報をキャプチャします。 |
| **show capture** | オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。 |

# pager

Telnet セッションで「---More---」プロンプトが表示されるまでの 1 ページあたりのデフォルト行数を設定するには、グローバル コンフィギュレーション モードで **pager** コマンドを使用します。

**pager** [**lines**] *lines*

## 構文の説明

| | |
|---|---|
| [**lines**] *lines* | 「---More---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページの制限がないことを示します。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは任意であり、このキーワードの有無にかかわらずコマンドは同一です。 |

## デフォルト

デフォルトは 24 行です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドは、特権 EXEC モードのコマンドからグローバル 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。**terminal pager** コマンドが、特権 EXEC モードのコマンドとして追加されました。 |

## 使用上のガイドライン

このコマンドは、Telnet セッションでのデフォルトの pager line 設定を変更します。現在のセッションについてのみ、設定を一時的に変更する場合は、**terminal pager** コマンドを使用します。

管理コンテキストに対して Telnet 接続し、他のコンテキストに変更した場合、そのコンテキストの **pager** コマンドで別の設定が使用される場合でも、pager line 設定はセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

## 例

次に、表示される行数を 20 に変更する例を示します。

```
ciscoasa(config)# pager 20
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure terminal** | 端末の表示幅設定をクリアします。 |
| **show running-config terminal** | 現在の端末設定を表示します。 |
| **terminal** | システム ログ メッセージを Telnet セッションで表示できるようにします。 |
| **terminal pager** | Telnet セッションで「`---more---`」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。 |
| **terminal width** | グローバル コンフィギュレーション モードでの端末の表示幅を設定します。 |

# page style

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **page style** 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て、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。

**page style** *value*

[**no**] **page style** *value*

## 構文の説明

| | |
|---|---|
| *value* | カスケーディング スタイル シート（CSS）パラメータ（最大 256 文字）。 |

## デフォルト

デフォルトのページ スタイルは、background-color:white;font-family:Arial,Helv,sans-serif です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

**style** オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

(注) WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

## 例

次に、ページ スタイルを large にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# page style font-size:large
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **logo** | WebVPN ページのロゴをカスタマイズします。 |
| **title** | WebVPN ページのタイトルをカスタマイズします。 |

# parameters

パラメータ コンフィギュレーション モードを開始してインスペクション ポリシー マップのパラメータを設定するには、ポリシー マップ コンフィギュレーション モードで **parameters** コマンドを使用します。

**パラメータ**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で、**inspect** コマンドを使用してインスペクション エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成されたインスペクション ポリシー マップで定義されているアクションを、オプションでイネーブルにすることもできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は、インスペクション ポリシー マップの名前です。

インスペクション ポリシー マップは、1 つ以上の **parameters** コマンドをサポートできます。パラメータは、インスペクション エンジンの動作に影響します。パラメータ コンフィギュレーション モードで使用できるコマンドは、アプリケーションによって異なります。

## 例

次に、デフォルトのインスペクション ポリシー マップにおける DNS パケットの最大メッセージ長を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 512
```

## 関連コマンド

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

# participate

デバイスを仮想ロードバランシング クラスタに強制参加させるには、VPN ロード バランシング コンフィギュレーション モードで **participate** コマンドを使用します。クラスタへの参加からデバイスを削除するには、このコマンドの **no** 形式を使用します。

**participate**

**no participate**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作では、デバイスは VPN ロード バランシング クラスタに参加しません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

まず、**interface** および **nameif** コマンドを使用してインターフェイスを設定し、**vpn load-balancing** コマンドを使用して VPN ロード バランシング モードを開始する必要があります。さらに、**cluster ip** コマンドを使用してクラスタ IP アドレスを設定し、仮想クラスタ IP アドレスが参照するインターフェイスを設定しておく必要があります。

このコマンドは、このデバイスを仮想ロード バランシング クラスタに強制的に参加させます。デバイスへの参加をイネーブルにするには、このコマンドを明示的に発行する必要があります。

クラスタに参加するすべてのデバイスは、IP アドレス、暗号設定、暗号キー、およびポートというクラスタ固有の同一値を共有する必要があります。

(注) 暗号化を使用するときは、**isakmp enable** *inside* コマンドをあらかじめ設定しておく必要があります。*inside* は、ロード バランシングの内部インターフェイスを指定します。ロード バランシングの内部インターフェイスで isakmp がイネーブルでない場合は、クラスタ暗号化を設定しようとするとエラー メッセージが表示されます。

isakmp が **cluster encryption** コマンドの設定時にはイネーブルで、**participate** コマンドを設定する前にディセーブルになった場合、**participate** コマンドを入力するとエラー メッセージが表示され、ローカル デバイスはクラスタに参加しません。

## 例

次に、現在のデバイスを VPN ロード バランシング クラスタに参加できるようにする **participate** コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

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

## 関連コマンド

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

# passive-interface（IPv6 ルータ OSPF）

特定のインターフェイスまたは OSPFv3 プロセスを使用しているすべてのインターフェイスでルーティング更新の送受信を行わないようにするには、IPv6 ルータ OSPF コンフィギュレーション モードで **passive-interface** コマンドを使用します。特定のインターフェイスまたは OSPFv3 プロセスを使用しているすべてのインターフェイスでルーティング更新を再び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。

**passive-interface** [*interface_name*]

**no passive-interface** [*interface_name*]

## 構文の説明

| | |
|---|---|
| *interface_name* | （オプション）OSPFv3 プロセスが実行されているインターフェイスの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| コマンド モード | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| | ルーテッド | トランスペアレント | シングル | コンテキスト | システム |
| IPv6 ルータ OSPF コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.0(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、インターフェイスでパッシブ ルーティングをイネーブルにします。

## 例

次に、内部インターフェイスでルーティング更新の送受信を行わないようにする例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# passive-interface interface
ciscoasa(config-rtr)#
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **show running-config router** | 実行コンフィギュレーションに含まれるルータ コンフィギュレーション コマンドを表示します。 |

# passive-interface（ISIS）

トポロジ データベースにまだインターフェイス アドレスが含まれている場合に、インターフェイスで ISIS hello パケットおよびルーティング アップデートを選択するには、ルータ ISIS コンフィギュレーション モードで **passive-interface** コマンドを使用します。発信 hello パケットおよびルーティング アップデートを再び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。

**passive-interface [default | inside | management | management2]**

**no passive-interface [default | inside | management | management2]**

## 構文の説明

| | |
|---|---|
| **default** | すべてのインターフェイス上でルーティングが更新されないようにします。 |
| **inside** | インターフェイス GigabithEthernet0/0 の名前。 |
| **管理** | インターフェイス Management0/0 の名前。 |
| **management2** | インターフェイス Management0/1 の名前。 |

## デフォルト

デフォルトでは、すべてのインターフェイス上でルーティングが更新されません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.6(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、インターフェイスでパッシブ ルーティングをイネーブルにします。

## 例

次に、内部インターフェイスでルーティング更新の送受信を行わないようにする例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# passive-interface inside
```

## 関連コマンド

# passive-interface（ルータ EIGRP）

インターフェイスで EIGRP ルーティング更新の送受信をディセーブルにするには、ルータ EIGRP コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスでルーティング更新を再び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。

**passive-interface** {**default** | *if_name*}

**no passive-interface** {**default** | *if_name*}

## 構文の説明

| | |
|---|---|
| **default** | （任意）すべてのインターフェイスを受動モードに設定します。 |
| *if_name* | （任意）**nameif** コマンドでパッシブ モードに指定したインターフェイスの名前。 |

## デフォルト

そのインターフェイスでルーティングがイネーブルになると、アクティブ ルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスがイネーブルになります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが追加されました。 |
| 8.0(2) | EIGRP ルーティングのサポートが追加されました。 |

## 使用上のガイドライン

インターフェイス上でパッシブ ルーティングをイネーブルにします。EIGRP の場合は、これによりそのインターフェイスでのルーティング更新の送受信がディセーブルになります。

EIGRP コンフィギュレーションでは、複数の **passive-interface** コマンドを使用できます。**passive-interface default** コマンドを使用してすべてのインターフェイスで EIGRP ルーティングをディセーブルにし、次に **no passive-interface** コマンドを使用して特定インターフェイスで EIGRP ルーティングをイネーブルにすることが可能です。

## 例

次に、外部インターフェイスをパッシブ EIGRP に設定する例を示します。セキュリティ アプライアンスの他のインターフェイスは、EIGRP 更新を送受信します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

次に、内部インターフェイスを除くすべてのインターフェイスをパッシブ EIGRP に設定する例を示します。内部インターフェイスのみが EIGRP 更新を送受信します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface default
ciscoasa(config-router)# no passive-interface inside
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show running-config router** | 実行コンフィギュレーションに含まれるルータ コンフィギュレーション コマンドを表示します。 |

# passive-interface（ルータ RIP）

インターフェイスで RIP ルーティング更新の送信をディセーブルにするには、ルータ RIP コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスで RIP ルーティング更新を再び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。

**passive-interface** {**default** | *if_name*}

**no passive-interface** {**default** | *if_name*}

## 構文の説明

| | |
|---|---|
| **default** | （任意）すべてのインターフェイスを受動モードに設定します。 |
| *if_name* | （任意）指定したインターフェイスをパッシブ モードに設定します。 |

## デフォルト

RIP がイネーブルになると、アクティブ RIP に対してすべてのインターフェイスがイネーブルになります。

インターフェイスまたは **default** キーワードを指定しない場合、コマンドのデフォルトは **default** であり、コンフィギュレーションでは passive-interface default として表示されます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

インターフェイス上でパッシブ RIP をイネーブルにします。インターフェイスは RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルを設定しますが、ルーティング更新はブロードキャストしません。

## 例

次に、外部インターフェイスをパッシブ RIP に設定する例を示します。セキュリティ アプライアンスの他のインターフェイスは、RIP 更新を送受信します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure rip** | 実行コンフィギュレーションからすべての RIP コマンドをクリアします。 |
| **router rip** | RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードを開始します。 |
| **show running-config rip** | 実行コンフィギュレーションの RIP コマンドを表示します。 |

# passwd、password

Telnet のログイン パスワードを設定するには、グローバル コンフィギュレーション モードで **passwd** または **password** コマンドを使用します。パスワードをリセットにするには、このコマンドの **no** 形式を使用します。

{**passwd** | **password**} *password* [**encrypted**]

**no** {**passwd** | **password**} *password*

## 構文の説明

| | |
|---|---|
| **encrypted** | (任意)パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由でパスワードを別の ASA にコピーする必要があるが、元のパスワードがわからない場合、暗号化されたパスワードとこのキーワードを指定して **passwd** コマンドを入力できます。通常、このキーワードは、**show running-config passwd** コマンドを入力するときにだけ表示されます。 |
| **passwd** \| **password** | どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。 |
| *password* | パスワードを最大 80 文字のストリングで設定します。大文字と小文字は区別されます。パスワードにスペースを含めることはできません。 |

## デフォルト

9.1(1):デフォルトのパスワードは「cisco」です。

9.1(2):デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 8.4(2) | SSH デフォルト ユーザ名がサポートされなくなり、**pix** または **asa** ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。 |

| リリース | 変更内容 |
|---|---|
| 9.0(2)、9.1(2) | デフォルトのパスワード「cisco」が削除され、ログイン パスワードを能動的に設定しなければならなくなりました。**no passwd** コマンドまたは **clear configure passwd** コマンドを使用した場合、以前のバージョンではパスワードがデフォルトの「cisco」にリセットされましたが、パスワードが削除されるようになりました。 |

## 使用上のガイドライン

**telnet** コマンドを使用して Telnet をイネーブルにする場合、**passwd** コマンドで設定したパスワードでログインできます。ログイン パスワードを入力すると、ユーザ EXEC モードが開始されます。**aaa authentication telnet console** コマンドを使用して Telnet のユーザごとに CLI 認証を設定する場合、このパスワードは使用されません。

このパスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。

## 例

次に、パスワードを Pa$$w0rd に設定する例を示します。

```
ciscoasa(config)# passwd Pa$$w0rd
```

次に、パスワードを別の ASA からコピーした暗号化されたパスワードに設定する例を示します。

```
ciscoasa(config)# passwd jMorNbK0514fadBh encrypted
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure passwd** | ログイン パスワードをクリアします。 |
| **enable** | 特権 EXEC モードを開始します。 |
| **イネーブル パスワード** | イネーブル パスワードを設定します。 |
| **show curpriv** | 現在ログインしているユーザ名とユーザの特権レベルを表示します。 |
| **show running-config passwd** | 暗号化された形式でログイン パスワードを表示します。 |

# password（クリプト CA トラストポイント）

登録時に CA に登録されたチャレンジ フレーズを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **password** 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。

**password** *string*

**no password**

## 構文の説明

| | |
|---|---|
| *string* | パスワードの名前をストリングとして指定します。最初の文字を数値にはできません。ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字-スペース-任意の文字の形式ではパスワードを指定できません。数字の後にスペースを使用すると、問題が発生します。たとえば、「hello 21」は有効なパスワードですが、「21 hello」は無効です。パスワード チェックでは、大文字と小文字が区別されます。たとえば、パスワード「Secret」とパスワード「secret」は異なります。 |

## デフォルト

デフォルト設定では、パスワードを含めません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

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

## 使用上のガイドライン

このコマンドを使用すると、実際の証明書登録を開始する前に、証明書失効パスワードを指定できます。指定されたパスワードは、更新されたコンフィギュレーションが ASA によって NVRAM に書き込まれるときに暗号化されます。

CA は、通常、チャレンジ フレーズを使用して、その後の失効要求を認証します。

このコマンドがイネーブルの場合、証明書登録時にパスワードを求められません。

## 例

次に、トラストポイント central に対してクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central に対する登録要求で CA に登録されたチャレンジ フレーズを指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# password zzxxyy
```

## 関連コマンド

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

# password encryption aes

マスター パスフレーズを使用してパスワードの暗号化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 **password encryption aes** コマンドを使用します。パスワードの暗号化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。

**password encryption aes**

**no password encryption aes**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.3(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

パスワードの暗号化をトリガーするには、**key config-key password-encrypt** コマンドと **password encryption aes** コマンドの両方を任意の順序で入力する必要があります。**write memory** と入力して、暗号化されたパスワードをスタートアップ コンフィギュレーションに保存します。そうしないと、スタートアップ コンフィギュレーション内のパスワードが表示されることがあります。マルチコンテキスト モードでは、システム実行スペースに **write memory all** を使用してすべてのコンテキストの設定を保存します。後から **no password encryption aes** コマンドを使用してパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードは変更されず、マスター パスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。

このコマンドを実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュア セッションにおいてのみです。

アクティブ/スタンバイ フェールオーバーでパスワード暗号化をイネーブルにするか、または変更すると、**write standby** が実行され、アクティブな設定をスタンバイ ユニットに複製することになります。この複製がないと、スタンバイ ユニット上の暗号化されたパスワードが、同じパスフレーズを使用していても、異なるものになります。設定の複製によって設定が同じになることが保証されます。アクティブ/アクティブ フェールオーバーの場合は、**write standby** と手動で入力する必要があります。アクティブ/アクティブ モードでは、**write standby** によってトラフィックの中断が発生します。これは、新しい設定が同期される前に、セカンダリ ユニットで設定がクリアされるためです。**failover active group 1** コマンドと **failover active group 2** コマンドを使用してプライマリ ASA のすべてのコンテキストをアクティブにし、**write standby** と入力してから、**no failover active group 2** コマンドを使用してグループ 2 のコンテキストをセカンダリ ユニットに復元します。

**write erase** コマンドに続いて **reload** コマンドを使用すると、マスターパスフレーズを紛失した場合はそのマスターパスフレーズとすべての設定が削除されます。

## 例

次に、暗号キーの生成に使用するパスフレーズを設定し、パスワード暗号化をイネーブルにする例を示します。

```
ciscoasa(config)# key config-key password-encryption
    Old key: bumblebee
    New key: haverford
    Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasahostname(config)# write memory
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **key config-key password-encryption** | 暗号キーの生成に使用されるパスフレーズを設定します。 |
| **write erase** | **reload** コマンドを続いて使用すると、マスター パスフレーズが紛失された場合にパスフレーズを削除します。 |

# password-history

このコマンドは、**password-policy reuse-interval** コマンドをイネーブルにしたときに **username attributes** コマンドの設定に表示されます。また、これはユーザによる設定が可能なコマンドではありません。以前のパスワードを暗号化された形式で保存します。

**password-history** *hash1,hash2,hash3 ...*

## 構文の説明

| | |
|---|---|
| *hash1,hash2,hash3, ...* | PBKDF2（パスワードベースのキー派生関数 2）を使用してハッシュされた以前のパスワードを表示します。 |

## コマンドデフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.8(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

これは、ユーザが設定できないコマンドであり、**password-policy reuse-interval** コマンドをイネーブルにした場合に show 出力にだけ表示されます。

## 例

次に、パスワードを 2 回変更してから以前のハッシュされたパスワードを表示する例を示します。

```
ciscoasa(config)# username test password pw1
ciscoasa(config)# show running-config username test
username test password $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
pbkdf2
ciscoasa(config)# username test password pw2
ciscoasa(config)# show running-config username test
username test password $sha512$5000$d8ebNCK2oTyzSiHjSh2T6w==$urDQ/+9sOPwi4IUftWFMcw==
pbkdf2
username test attributes
  password-history $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
ciscoasa(config)# username test password pw3
ciscoasa(config)# show running-config username test
```

```
username test password $sha512$5000$o8WLa1qnLdp2Js4OlW+NdQ==$4Be4eHtPmOxdpfH6j+F4qQ==
pbkdf2
username test attributes
  password-history
$sha512$5000$d8ebNCK2oTyzSiHjSh2T6w==$urDQ/+9sOPwi4IUftWFMcw==,$sha512$5000$4tAPQTnL3WG1aa
4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
ciscoasa(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa authentication login-history** | ローカル **username** のログイン履歴を保存します。 |
| **password-policy reuse-interval** | **username** パスワードの再利用を禁止します。 |
| **password-policy username-check** | **username** の名前と一致するパスワードを禁止します。 |
| **show aaa login-history** | ローカル **username** のログイン履歴を表示します。 |
| **username** | ローカル ユーザを設定します。 |

# password-management

パスワード管理をイネーブルにするには、トンネル グループ一般属性コンフィギュレーション モードで **password-management** コマンドを使用します。パスワード管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。日数をデフォルト値にリセットするには、このコマンドの **no** 形式を使用し、**password-expire-in-days** キーワードを指定します。

**password-management** [**password-expire-in-days** *days*]

**no password-management**

**no password-management password-expire-in-days** [*days*]

## 構文の説明

| | |
|---|---|
| *days* | 現行のパスワードが失効するまでの日数(0 ～ 180)を指定します。**password-expire-in-days** キーワードを指定する場合は、このパラメータは必須です。 |
| **password-expire-in-days** | (任意)直後のパラメータが、ASA でユーザに対して失効が迫っている警告を開始してから、現行のパスワードが失効するまでの日数を指定していることを示します。このオプションは、LDAP サーバに対してのみ有効です。詳細については、「Usage Notes」を参照してください。 |

## デフォルト

デフォルトでは、パスワード管理は行われません。LDAP サーバに対して **password-expire-in-days** キーワードを指定しない場合、現行のパスワードが失効する前に警告を開始するデフォルトの期間は、14 日です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

ASA では、RADIUS および LDAP プロトコルのパスワード管理をサポートします。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPsec リモート アクセスと SSL VPN トンネルグループのパスワード管理を設定できます。

password-management コマンドを設定すると、ASA は、リモート ユーザがログインするときに、そのユーザの現在のパスワードの期限切れが迫っている、または期限が切れたことを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このコマンドは、それらの通知をサポートする AAA サーバ、つまりネイティブの LDAP サーバおよび RADIUS プロキシとして構成された NT 4.0 または Active Directory サーバに対して有効です。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

(注) MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。

ASA のリリース 7.1 以降では通常、LDAP による認証時、または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント（ASA ソフトウェア バージョン 8.0 以降）
- IPsec VPN クライアント
- クライアントレス SSL VPN（ASA ソフトウェア バージョン 8.0 以降）、WebVPN（ASA ソフトウェア バージョン 7.1 ～ 7.2.x）
- SSL VPN フル トンネル クライアント

これらの RADIUS 設定には、ローカル認証の RADIUS、Active Directory/Kerberos Windows DC の RADIUS、NT/4.0 ドメインの RADIUS、LDAP の RADIUS が含まれます。

Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポート*されません*。RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバのみに対して通信しているように見えます。

(注) LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。

ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

このコマンドは、パスワードが失効するまでの日数を変更するものではなく、ASA がユーザに対してパスワード失効の警告を開始してから失効するまでの日数を変更するものである点に注意してください。

**password-expire-in-days** キーワードを指定する場合は、日数も指定する必要があります。

このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。ASA は、ユーザに対して失効が迫っていることを通知しませんが、失効後にユーザはパスワードを変更できます。

(注) RADIUS では、パスワードが変更されることも、パスワードの変更を求められることもありません。

## 例

次に、WebVPN トンネル グループ「testgroup」について、ユーザに対して失効が迫っている警告を開始してからパスワードが失効するまでの日数を 90 に設定する例を示します。

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# password-management password-expire-in-days 90
ciscoasa(config-tunnel-general)#
```

次に、IPsec リモート アクセス トンネル グループ「QAgroup」について、ユーザに対して失効が迫っている警告を開始してからパスワードが失効するまでの日数としてデフォルトの 14 日を使用する例を示します。

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# password-management
ciscoasa(config-tunnel-general)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure passwd** | ログイン パスワードをクリアします。 |
| **passwd** | ログイン パスワードを設定します。 |
| **radius-with-expiry** | RADIUS 認証時のパスワード更新のネゴシエーションをイネーブルにします(廃止)。 |
| **show running-config passwd** | 暗号化された形式でログイン パスワードを表示します。 |
| **tunnel-group general-attributes** | トンネル グループ一般属性値を設定します。 |

# password-parameter

SSO 認証用のユーザ パスワードを送信する HTTP POST 要求パラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **password-parameter** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。

**password-parameter** *string*

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

## 構文の説明

| | |
|---|---|
| *string* | HTTP POST 要求に含まれるパスワード パラメータの名前。パスワードの最大長は 128 文字です。 |

## デフォルト

デフォルトの値や動作はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

ASA の WebVPN サーバは、HTTP POST 要求を使用して、認証 Web サーバにシングル サインオン認証要求を送信します。必須のコマンド **password-parameter** では、POST 要求に SSO 認証用のユーザ パスワード パラメータを含める必要があることを指定します。

(注) ユーザは、ログイン時に実際のパスワード値を入力します。このパスワード値は POST 要求に入力され、認証 Web サーバに渡されます。

## 例

次に、AAA サーバ ホスト コンフィギュレーション モードで、user_password という名前のパスワード パラメータを指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# password-parameter user_password
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **action-uri** | シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。 |
| **auth-cookie-name** | 認証クッキーの名前を指定します。 |
| **hidden-parameter** | 認証 Web サーバと交換するための非表示パラメータを作成します。 |
| **start-url** | プリログイン クッキーを取得する URL 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。 |

# password-policy authenticate enable

各自のユーザ アカウントの変更をユーザに許可するかどうかを指定するには、グローバル コンフィギュレーション モードで **password-policy authenticate enable** コマンドを使用します。対応するパスワード ポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**password-policy authenticate enable**

**no password-policy authenticate enable**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

認証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

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

認証がイネーブルの場合、ユーザが **username** コマンドを使用して各自のパスワードを変更したりアカウントを削除したりすることはできません。また、**clear configure username** コマンドを使用して各自のアカウントを削除することもできません。

## 例

次に、各自のユーザ アカウントの変更をユーザに許可する例を示します。

```
ciscoasa(config)# password-policy authenticate enable
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **password-policy minimum-changes** | 新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。 |
| **password-policy minimum length** | パスワードの最小長を設定します。 |
| **password-policy minimum-lowercase** | パスワードに含める小文字の最小個数を設定します。 |

# password-policy lifetime

現在のコンテキストのパスワード ポリシーおよびパスワードの有効期間（日数）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 **password-policy lifetime** コマンドを使用します。対応するパスワード ポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**password-policy lifetime** *value*

**no password-policy lifetime** *value*

## 構文の説明

| | |
|---|---|
| *value* | パスワードの有効期間を指定します。有効な値の範囲は、0 ～ 65535 日です。 |

## デフォルト

有効期間のデフォルト値は 0 日です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

パスワードには有効期間が指定されています。有効期間の値が 0 日の場合、ローカル ユーザのパスワードは期限切れになりません。ライフタイム有効期間の翌日の AM 12:00 にパスワードの期限が切れることに注意してください。

## 例

次に、パスワードの有効期間の値を 10 日に設定する例を示します。

```
ciscoasa(config)# password-policy lifetime 10
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **password-policy minimum-changes** | 新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。 |
| **password-policy minimum length** | パスワードの最小長を設定します。 |
| **password-policy minimum-lowercase** | パスワードに含める小文字の最小個数を設定します。 |

# password-policy minimum-changes

新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-changes** コマンドを使用します。対応するパスワード ポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**password-policy minimum-changes** *value*

**no password-policy minimum-changes** *value*

## 構文の説明

| | |
|---|---|
| *value* | 新規のパスワードと古いパスワードとの間で変更しなければならない文字数を指定します。有効値の範囲は 0 ～ 64 文字です。 |

## デフォルト

デフォルトの変更文字数は 0 文字です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

新しいパスワードには、現在のパスワードから少なくとも 4 文字は変更される必要があり、現在のパスワードの一部に新しいパスワードが含まれない場合のみ変更されたと見なされます。

## 例

次に、古いパスワードと新規のパスワードとの間の最小変更文字数を 6 文字に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-changes 6
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **password-policy lifetime** | パスワードの有効期間(日数)を設定します。 |
| **password-policy minimum-length** | パスワードの最小長を設定します。 |
| **password-policy minimum-lowercase** | パスワードに含める小文字の最小個数を設定します。 |

# password-policy minimum-length

パスワードの最小長を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-length** コマンドを使用します。対応するパスワード ポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**password-policy minimum-length** *value*

**no password-policy minimum-length** *value*

構文の説明

| | |
|---|---|
| *value* | パスワードの最小長を指定します。有効値の範囲は 3 ～ 32 文字です。 |

## デフォルト

デフォルトの最小長は 3 文字です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

最小長がその他の最小文字数の属性（変更文字、小文字、大文字、数字、特殊文字）の値よりも小さい場合、エラー メッセージが表示され、最小長の値は変更されません。推奨されるパスワードの長さは 8 文字です。

## 例

次に、パスワードの最小文字数を 8 文字に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-length 8
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **password-policy lifetime** | パスワードの有効期間の値（日数）を設定します。 |
| **password-policy minimum-changes** | 古いパスワードと新規のパスワードとの間の最小変更文字数を設定します。 |
| **password-policy minimum-lowercase** | パスワードに含める小文字の最小個数を設定します。 |

# password-policy minimum-lowercase

パスワードに含める小文字の最小個数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-lowercase** コマンドを使用します。対応するパスワード ポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**password-policy minimum-lowercase** *value*

**no password-policy minimum-lowercase** *value*

## 構文の説明

| | |
|---|---|
| *value* | パスワードで使用される小文字の最小個数を指定します。有効値の範囲は 0 ～ 64 文字です。 |

## デフォルト

小文字の最小個数のデフォルト値は 0 で、小文字を含める必要はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、パスワードに含める小文字の最小個数を設定します。有効値の範囲は 0 ～ 64 文字です。

## 例

次に、パスワードに含める小文字の最小個数を 6 個に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **password-policy lifetime** | パスワードの有効期間の値（日数）を設定します。 |
| **password-policy minimum-changes** | 新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。 |
| **password-policy minimum-length** | パスワードの最小長を設定します。 |

# password-policy minimum-numeric

パスワードに含める数字の最小個数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-numeric** コマンドを使用します。対応するパスワード ポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**password-policy minimum-numeric** *value*

**no password-policy minimum-numeric** *value*

## 構文の説明

| | |
|---|---|
| *value* | パスワードで使用される数字の最小個数を指定します。有効値の範囲は 0 ～ 64 文字です。 |

## デフォルト

数字の最小個数のデフォルト値は 0 で、数字を含める必要はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、パスワードに含める数字の最小個数を設定します。有効値の範囲は 0 ～ 64 文字です。

## 例

次に、パスワードに含める数字の最小個数を 8 個に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-numeric 8
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **password-policy lifetime** | パスワードの有効期間の値（日数）を設定します。 |
| **password-policy minimum-changes** | 新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。 |
| **password-policy minimum-length** | パスワードの最小長を設定します。 |

# password-policy minimum-special

パスワードに含める特殊文字の最小個数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-special** コマンドを使用します。対応するパスワード ポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**password-policy minimum-special** *value*

**no password-policy minimum-special** *value*

## 構文の説明

| | |
|---|---|
| *value* | パスワードで使用される特殊文字の最小個数を指定します。有効値の範囲は 0 ～ 64 文字です。 |

## デフォルト

特殊文字の最小個数のデフォルト値は 0 で、特殊文字を含める必要はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、パスワードに含める特殊文字の最小個数を設定します。特殊文字には、!、@、#、$、%、^、&、*、(、および )。

## 例

次に、パスワードに含める特殊文字の最小個数を 2 個に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-special 2
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **password-policy lifetime** | パスワードの有効期間の値（日数）を設定します。 |
| **password-policy minimum-changes** | 新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。 |
| **password-policy minimum-length** | パスワードの最小長を設定します。 |

# password-policy minimum-uppercase

パスワードに含める大文字の最小個数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-uppercase** コマンドを使用します。対応するパスワード ポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**password-policy minimum-uppercase** *value*

**no password-policy minimum-uppercase** *value*

## 構文の説明

| | |
|---|---|
| *value* | パスワードで使用される大文字の最小個数を指定します。有効値の範囲は 0 ～ 64 文字です。 |

## デフォルト

大文字の最小個数のデフォルト値は 0 で、大文字を含める必要はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、パスワードに含める大文字の最小個数を設定します。有効値の範囲は 0 ～ 64 文字です。

## 例

次に、パスワードに含める大文字の最小個数を 4 個に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-uppercase 4
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **password-policy lifetime** | パスワードの有効期間の値（日数）を設定します。 |
| **password-policy minimum-changes** | 新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。 |
| **password-policy minimum-length** | パスワードの最小長を設定します。 |

# password-policy reuse-interval

ローカル ユーザ名へのパスワードの再利用を禁止するには、グローバル コンフィギュレーション モードで **password-policy reuse-interval** コマンドを使用します。この制限を削除するには、このコマンドの **no** 形式を使用します。

**password-policy reuse-interval** *value*

**no password-policy reuse-interval** [*value*]

## 構文の説明

| | |
|---|---|
| *value* | 新しいパスワードを作成するときに使用できない以前のパスワードの数を 2 ～ 7 で設定します。 |

## コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.8(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

以前に使用したパスワードと一致しているパスワードの再利用を禁止できます。以前のパスワードは、**password-history** コマンドを使用して暗号化された形式で各 **username** の設定に保存されます。このコマンドをユーザが設定することはできません。

## 例

次に、パスワード再利用間隔を 5 に設定する例を示します。

```
ciscoasa(config)# password-policy reuse-interval 5
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa authentication login-history** | ローカル **username** のログイン履歴を保存します。 |
| **password-history** | 直前の **username** パスワードを保存します。ユーザはこのコマンドを設定できません。 |
| **password-policy username-check** | **username** の名前と一致するパスワードを禁止します。 |
| **show aaa login-history** | ローカル **username** のログイン履歴を表示します。 |
| **username** | ローカル ユーザを設定します。 |

# password-policy username-check

ユーザ名と一致するパスワードを禁止するには、グローバル コンフィギュレーション モードで **password-policy username-check** コマンドを使用します。この制限を削除するには、このコマンドの **no** 形式を使用します。

**password-policy username-check**

**no password-policy username-check**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.8(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

**username** コマンドの名前と一致するパスワードを禁止できます。

## 例

次に、ユーザ名の john_crichton に一致しないようにパスワードを制限する例を示します。

```
ciscoasa(config)# password-policy username-check
ciscoasa(config)# username john_crichton password moya privilege 15
ciscoasa(config)# username aeryn_sun password john_crichton privilege 15
ERROR: Password must contain:
ERROR: a value that complies with the password policy
ERROR: Username addition failed.
ciscoasa(config)#
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa authentication login-history** | ローカル **username** のログイン履歴を保存します。 |
| **password-history** | 直前の **username** パスワードを保存します。ユーザはこのコマンドを設定できません。 |
| **password-policy reuse-interval** | **username** パスワードの再利用を禁止します。 |
| **show aaa login-history** | ローカル **username** のログイン履歴を表示します。 |
| **username** | ローカル ユーザを設定します。 |

# password-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **password-prompt** コマンドを使用します。

**password-prompt** {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、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。

## 構文の説明

| | |
|---|---|
| **text** | テキストを変更することを指定します。 |
| **style** | スタイルを変更することを指定します。 |
| *value* | 実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。 |

## デフォルト

パスワード プロンプトのデフォルト テキストは、「PASSWORD:」です。

パスワード プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | トランスペアレント | シングル | コンテキスト | システム |
| WebVPN カスタマイゼーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

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

## 使用上のガイドライン

**style** オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

## 例

次に、テキストを「Corporate Password:」に変更し、フォントのウェイトを太くするようにデフォルト スタイルを変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# password-prompt text Corporate Username:
ciscoasa(config-webvpn-custom)# password-prompt style font-weight:bolder
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **group-prompt** | WebVPN ページのグループ プロンプトをカスタマイズします。 |
| **username-prompt** | WebVPN ページのユーザ名プロンプトをカスタマイズします。 |

# password-storage

ユーザがクライアント システムに各自のログイン パスワードを保管できるようにするには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **password-storage enable** コマンドを使用します。パスワードの保管をディセーブルにするには、**password-storage disable** コマンドを使用します。

実行コンフィギュレーションから password-storage 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーから password-storage 値を継承できます。

**password-storage {enable | disable}**

**no password-storage**

## 構文の説明

| | |
|---|---|
| **disable** | パスワードの保管をディセーブルにします。 |
| **enable** | パスワードの保管をイネーブルにします。 |

## デフォルト

パスワードの保管はディセーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

セキュア サイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。

このコマンドは、ハードウェア クライアントのインタラクティブ ハードウェア クライアント認証または個別ユーザ認証には関係ありません。

## 例

次に、FirstGroup という名前のグループ ポリシーに対してパスワードの保管をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# password-storage enable
```

# peer-id-validate

ピアの証明書を使用してピアの ID を検証するかどうかを指定するには、トンネル グループ IPSec 属性モードで **peer-id-validate** 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。

**peer-id-validate** *option*

**no peer-id-validate**

## 構文の説明

| | |
|---|---|
| *オプション* | 次のいずれかのオプションを指定します。<br>• **req**：必須<br>• **cert**：証明書でサポートされる場合<br>• **nocheck**：チェックしない |

## デフォルト

このコマンドのデフォルト設定は、**req** です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

この属性は、すべての IPsec トンネル グループ タイプに適用できます。

## 例

次に、設定 IPsec コンフィギュレーション モードで、209.165.200.225 という名前の IPsec LAN-to-LAN トンネル グループ用のピア証明書の ID を使用してピアの検証を要求する例を示します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPsec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# peer-id-validate req
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **clear-configure tunnel-group** | 設定されているすべてのトンネル グループをクリアします。 |
| **show running-config tunnel-group** | すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group ipsec-attributes** | このグループのトンネル グループ ipsec 属性を設定します。 |

# peer ip

ピア VXLAN トンネル エンドポイント(VTEP)の IP アドレスを手動で指定するには、NVE コンフィギュレーション モードで **peer ip** コマンドを使用します。ピア アドレスを削除するには、このコマンドの **no** 形式を使用します。

**peer ip** *ip_address*

**no peer ip**

## 構文の説明

| | |
|---|---|
| *ip_address* | ピア VTEP の IP アドレスを設定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、マルチ コンテキスト モードではサポートされていないため、手動設定が唯一のオプションです。VTEP には 1 つのピアのみを指定できます。

## 例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、ピア IPアドレス 10.1.1.2 を指定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **debug vxlan** | VXLAN トラフィックをデバッグします。 |
| **default-mcast-group** | VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。 |
| **encapsulation vxlan** | NVE インスタンスを VXLAN カプセル化に設定します。 |
| **inspect vxlan** | 標準 VXLAN ヘッダー形式に強制的に準拠させます。 |
| **interface vni** | VXLAN タギング用の VNI インターフェイスを作成します。 |
| **mcast-group** | VNI インターフェイスのマルチキャスト グループ アドレスを設定します。 |
| **nve** | ネットワーク仮想化エンドポイント インスタンスを指定します。 |
| **nve-only** | VXLAN 送信元インターフェイスが NVE 専用であることを指定します。 |
| **segment-id** | VNI インターフェイスの VXLAN セグメント ID を指定します。 |
| **show arp vtep-mapping** | リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。 |
| **show interface vni** | VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。 |
| **show mac-address-table vtep-mapping** | リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。 |
| **show nve** | NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。 |
| **show vni vlan-mapping** | VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。 |
| **source-interface** | VTEP 送信元インターフェイスを指定します。 |
| **vtep-nve** | VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。 |
| **vxlan port** | VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。 |

# perfmon

パフォーマンス情報を表示するには、特権 EXEC モードで **perfmon** コマンドを使用します。

**perfmon** {**verbose** | **interval** *seconds* | **quiet** | **settings**} [*detail*]

## 構文の説明

| | |
|---|---|
| **verbose** | パフォーマンス モニタ情報を ASA コンソールに表示します。 |
| **interval** *seconds* | コンソールでパフォーマンス表示がリフレッシュされるまでの秒数を指定します。 |
| **quiet** | パフォーマンス モニタ表示をディセーブルにします。 |
| **設定** | 間隔、および quiet と verbose のどちらであるかを表示します。 |
| *detail* | パフォーマンスに関する詳細情報を表示します。 |

## デフォルト

*seconds* は 120 秒です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | ASA でこのコマンドのサポートが追加されました。 |
| 7.2(1) | **detail** キーワードのサポートが追加されました。 |

## 使用上のガイドライン

**perfmon** コマンドを使用すると、ASA のパフォーマンスをモニタできます。**show perfmon** コマンドを使用すると、ただちに情報が表示されます。**perfmon verbose** コマンドを使用すると、2 分間隔で継続して情報が表示されます。**perfmon interval** *seconds* コマンドと **perfmon verbose** コマンドを組み合わせて使用すると、指定した秒数の間隔で継続して情報が表示されます。

次に、パフォーマンス情報の表示例を示します。

| PERFMON STATS: | Current | Average |
|---|---|---|
| Xlates | 33/s | 20/s |
| Connections | 110/s | 10/s |
| TCP Conns | 50/s | 42/s |
| WebSns Req | 4/s | 2/s |
| TCP Fixup | 20/s | 15/s |

| | | |
|---|---|---|
| HTTP Fixup | 5/s | 5/s |
| FTP Fixup | 7/s | 4/s |
| AAA Authen | 10/s | 5/s |
| AAA Author | 9/s | 5/s |
| AAA Account | 3/s | 3/s |

この情報には、毎秒発生する変換数、接続数、Websense 要求数、アドレス変換数（フィックスアップ数）、AAA トランザクション数が示されます。

## 例

次に、パフォーマンス モニタ統計情報を 30 秒間隔で ASA コンソールに表示する例を示します。

```
ciscoasa(config)# perfmon interval 120
ciscoasa(config)# perfmon quiet
ciscoasa(config)# perfmon settings
interval: 120 (seconds)
quiet
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show perfmon** | パフォーマンス情報を表示します。 |

# periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、時間範囲コンフィギュレーション モードで **periodic** コマンドを使用します。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。

**periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*

**no periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*

## 構文の説明

| | |
|---|---|
| days-of-the-week | （任意）1 番めの days-of-the-week 引数は、関連付けられている時間範囲の有効範囲が開始する日または曜日です。2 番めの days-of-the-week 引数は、関連付けられているステートメントの有効期間が終了する日または曜日です。<br>この引数は、単一の曜日または曜日の組み合わせです（Monday（月曜日）、Tuesday（火曜日）、Wednesday（水曜日）、Thursday（木曜日）、Friday（金曜日）、Saturday（土曜日）、および Sunday（日曜日））。他に指定できる値は、次のとおりです。<br>• daily：月曜日～日曜日<br>• weekdays：月曜日～金曜日<br>• weekend：土曜日と日曜日<br>終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。 |
| *時刻* | 時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。 |
| **to** | 「開始時刻から終了時刻まで」の範囲を入力するには、**to** キーワードを入力する必要があります。 |

## デフォルト

**periodic** コマンドで値を入力しない場合は、ASA へのアクセスが **time-range** コマンドで定義されたとおりにただちに有効になり、常に有効になります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドとともに使用して、時間範囲を ACL にバインドします。

**periodic** コマンドは、時間範囲が有効になるタイミングを指定する 1 つの方法です。**absolute** コマンドを使用して絶対時間範囲を指定する、という別の方法もあります。**time-range** グローバル コンフィギュレーション コマンドで時間範囲の名前を指定した後に、これらのコマンドのいずれかを使用します。**time-range** コマンド 1 つあたり複数の **periodic** エントリを使用できます。

終了の days-of-the-week 値が開始の days-of-the-week 値と同じ場合、終了の days-of-the-week 値を省略できます。

**time-range** コマンドに **absolute** 値と **periodic** 値の両方が指定されている場合、**periodic** コマンドは **absolute start** 時刻を経過した後にのみ評価の対象になり、**absolute end** 時刻を経過した後は評価の対象にはなりません。

時間範囲機能は、ASA のシステム クロックに依存しています。ただし、この機能は NTP 同期を使用すると最適に動作します。

## 例

次に例をいくつか示します。

| 必要な設定 | 入力内容 |
|---|---|
| 月曜日から金曜日の午前 8:00 ～午後 6:00 のみ | **periodic weekdays 8:00 to 18:00** |
| 毎日午前 8:00 ～午後 6:00 のみ | **periodic daily 8:00 to 18:00** |
| 月曜日午前 8:00 ～金曜日午後 8:00 の 1 分おき | **periodic monday 8:00 to friday 20:00** |
| 週末（土曜日の朝～日曜日の夜） | **periodic weekend 00:00 to 23:59** |
| 土曜日と日曜日の正午～深夜 | **periodic weekend 12:00 to 23:59** |

次に、月曜日から金曜日の午前 8:00 ～午後 6:00 のみ、ASA へのアクセスを許可する例を示します。

```
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
ciscoasa(config-time-range)#
```

次に、特定の曜日（月曜日、火曜日、および金曜日）の午前 10:30 ～午後 12:30 に、ASA へのアクセスを許可する例を示します。

```
ciscoasa(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
ciscoasa(config-time-range)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **absolute** | 時間範囲が有効になる絶対時間を定義します。 |
| access-list extended | ASA 経由の IP トラフィックを許可または拒否するためのポリシーを設定します。 |
| **default** | **time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。 |
| **time-range** | 時間に基づいて ASA のアクセス コントロールを定義します。 |

# periodic-authentication certificate

定期的な証明書の検証をイネーブルにするには、**periodic-authentication certificate** コマンドを使用します。デフォルトのグループ ポリシーから設定を継承するには、このコマンドの **no** 形式を使用します。

**periodic-authentication certificate <*time in hours*> | none**

**[no] periodic-authentication certificate <*time in hours*> | none**

## 構文の説明

| | |
|---|---|
| *time in hours* | 間隔（1 ～ 168 時間）を設定します。 |
| **none** | 定期的な認証がディセーブルになります。 |

## デフォルト

デフォルトでは、定期的な証明書の検証はディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

デフォルト グループ ポリシーの場合、このコマンドはデフォルトで **periodic-authentication certificate none** になります。他のグループ ポリシーの場合は、変更されないかぎり、デフォルト ポリシーから設定が継承されます。

## 例

```
100(config-group-policy)# periodic-authentication ?

group-policy mode commands/options:
  certificate  Configure periodic certificate authentication

100(config-group-policy)# periodic-authentication certificate ?

group-policy mode commands/options:
  <1-168>  Enter periodic authentication interval in hours
  none     Disable periodic authentication
```

```
100(config-group-policy)# periodic-authentication certificate ?

group-policy mode commands/options:
  <1-168>  Enter periodic authentication interval in hours
  none     Disable periodic authentication

100(config-group-policy)# help periodic-authentication
```

# permit-errors

無効な GTP パケットを許可するか、または許可しないと解析が失敗してドロップされるパケットを許可するには、ポリシー マップ パラメータ コンフィギュレーション モードで **permit-errors** コマンドを使用します。デフォルトの動作（無効なパケットまたは解析中に失敗したパケットをすべてドロップする）に戻すには、このコマンドの **no** 形式を使用します。

**permit-errors**

**no permit-errors**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトでは、無効なパケットまたは解析時に失敗したパケットはすべてドロップされます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

GTP インスペクション ポリシー マップ パラメータで **permit-errors** コマンドを使用すると、無効なパケットやメッセージのインスペクション中にエラーが発生したパケットをドロップするのではなく、ASA 経由で送信することができます。

## 例

次に、無効なパケットや解析中に失敗したパケットを含むトラフィックを許可する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# permit-errors
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **policy-map type inspect gtp** | GTP インスペクション ポリシー マップを定義します。 |
| **inspect gtp** | アプリケーション インスペクションに使用する特定の GTP マップを適用します。 |

# permit-response

GSN または PGW プーリングを設定するには、ポリシー マップ パラメータ コンフィギュレーション モードで **permit-response** コマンドを使用します。プーリング関係を削除するには、このコマンドの **no** 形式を使用します。

**permit-response to-object-group** *to_obj_group_id* **from-object-group** *from_obj_group_id*

**no permit-response to-object-group** *to_obj_group_id* **from-object-group** *from_obj_group_id*

## 構文の説明

| | |
|---|---|
| **from-object-group** *from_obj_group_id* | GSN/PGW エンドポイントを識別するネットワーク オブジェクト グループ。これは、オブジェクト グループ（**object-group** コマンド）である必要があります。これらのエンドポイントは、**to-object-group** に対して要求を送信し、応答を受信することが許可されます。<br>リリース 9.5(1) 以降では、オブジェクト グループは、IPv4 アドレスだけでなく IPv6 アドレスを含むことができます。 |
| **to-object-group** *to_obj_group_id* | SGSN/SGW を識別するネットワーク オブジェクト グループ。これは、オブジェクト グループ（**object-group** コマンド）である必要があります。これらのアドレスは、**from-object-group** で識別される一連のエンドポイントから応答を受信することが許可されます。<br>リリース 9.5(1) 以降では、オブジェクト グループは、IPv4 アドレスだけでなく IPv6 アドレスを含むことができます。 |

## デフォルト

ASA は、GTP 要求で指定されていない GSN または PGW からの GTP 応答をドロップします。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 (4) | このコマンドが追加されました。GTP インスペクションは IPv4 アドレスのみをサポートします。 |
| 9.5(1) | IPv6 アドレスのサポートが追加されました。 |

## 使用上のガイドライン

ASA が GTP インスペクションを実行する場合、デフォルトで ASA は、GTP 要求で指定されていない GSN または PGW からの GTP 応答をドロップします。これは、GSN または PGW のプール間でロードバランシングを使用して、GPRS の効率とスケーラビリティを高めているときに発生します。

GSN/PGW プーリングを設定し、ロード バランシングをサポートするために、GSN/PGW エンドポイントを指定するネットワーク オブジェクト グループを作成し、これを from-object-group パラメータで指定します。同様に、SGSN/SGW のネットワーク オブジェクト グループを作成し、to-object-group パラメータで選択します。応答を行う GSN/PGW が GTP 要求の送信先 GSN/PGW と同じオブジェクト グループに属しており、応答している GSN/PGW による GTP 応答の送信が許可されている先のオブジェクト グループに SGSN/SGW がある場合に、ASA で応答が許可されます。

ネットワーク オブジェクト グループは、エンドポイントをホスト アドレスまたはエンドポイントを含むサブネットから識別できます。

## 例

次に、192.168.32.0 ネットワーク上の任意のホストから IP アドレス 192.168.112.57 のホストへの GTP 応答を許可する例を示します。

```
ciscoasa(config)# object-group network gsnpool32
ciscoasa(config-network)# network-object 192.168.32.0 255.255.255.0
ciscoasa(config)# object-group network sgsn1
ciscoasa(config-network)# network-object host 192.168.112.57
ciscoasa(config-network)# exit
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# permit-response to-object-group sgsn1 from-object-group gsnpool32
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **policy-map type inspect gtp** | GTP インスペクション ポリシー マップを定義します。 |
| **inspect gtp** | アプリケーション インスペクションに使用する特定の GTP マップを適用します。 |
| **show service-policy inspect gtp** | GTP コンフィギュレーションを表示します。 |

# pfs

PFS をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **pfs enable** コマンドを使用します。PFS をディセーブルにするには、**pfs disable** コマンドを使用します。実行コンフィギュレーションから PFS 属性を削除するには、このコマンドの **no** 形式を使用します。

**pfs {enable | disable}**

**no pfs**

## 構文の説明

| | |
|---|---|
| **disable** | PFS をディセーブルにします。 |
| **enable** | PFS をイネーブルにします。 |

## デフォルト

PFS はディセーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

VPN クライアントと ASA の PFS 設定は一致する必要があります。

別のグループ ポリシーから PFS の値を継承できるようにするには、このコマンドの **no** 形式を使用します。

IPsec ネゴシエーションでは、PFS によって、新しい各暗号キーが以前のいずれのキーとも関連しないことが保証されます。

## 例

次に、FirstGroup という名前のグループ ポリシーに対して PFS を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# pfs enable
```

# phone-proxy（廃止）

電話プロキシ インスタンスを設定するには、グローバル コンフィギュレーション モードで **phone-proxy** コマンドを使用します。

電話プロキシ インスタンスを削除するには、このコマンドの **no** 形式を使用します。

**phone-proxy** *phone_proxy_name*

**no phone-proxy** *phone_proxy_name*

## 構文の説明

| | |
|---|---|
| *phone_proxy_name* | Phone Proxy インスタンスの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(4) | コマンドが追加されました。 |
| 9.4(1) | このコマンドは廃止されました。 |

## 使用上のガイドライン

ASA では、電話プロキシ インスタンスを 1 つだけ設定できます。

HTTP プロキシ サーバ用に NAT が設定されている場合、IP 電話に関する HTTP プロキシ サーバのグローバルまたはマッピング IP アドレスは、電話プロキシ コンフィギュレーション ファイルに書き込まれます。

## 例

次に、**phone-proxy** コマンドを使用して、電話プロキシ インスタンスを設定する例を示します。

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
ciscoasa(config-phone-proxy)# media-termination address 192.0.2.25 interface inside
ciscoasa(config-phone-proxy)# media-termination address 128.106.254.3 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa(config-phone-proxy)# ctl-file asactl
```

```
ciscoasa(config-phone-proxy)# cluster-mode nonsecure
ciscoasa(config-phone-proxy)# timeout secure-phones 00:05:00
ciscoasa(config-phone-proxy)# disable service-settings
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ctl-file（グローバル）** | Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。 |
| **ctl-file（Phone-Proxy）** | Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。 |
| **tls-proxy** | TLS プロキシ インスタンスを設定します。 |

# pim

インターフェイス上で PIM を再びイネーブルにするには、インターフェイス コンフィギュレーション モードで **pim** コマンドを使用します。PIM 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。

**pim**

**no pim**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM をイネーブルにします。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM をイネーブルにします。**pim** コマンドの **no** 形式のみが、コンフィギュレーションに保存されます。

**（注）** PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

## 例

次に、選択したインターフェイスで PIM をディセーブルにする例を示します。

```
ciscoasa(config-if)# no pim
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# pim accept-register

PIM 登録メッセージをフィルタリングするように ASA 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 **pim accept-register** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

**pim accept-register** {**list** *acl* | **route-map** *map-name*}

**no pim accept-register**

## 構文の説明

| | |
|---|---|
| **list** *acl* | アクセス リストの名前または番号を指定します。このコマンドでは、拡張ホスト ACL のみを使用します。 |
| **route-map** *map-name* | ルート マップ名を指定します。参照されるルート マップでは、拡張ホスト ACL を使用します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

このコマンドは、不正な送信元を RP に登録できないようにするために使用します。不正な送信元が RP に登録メッセージを送信すると、ASA はただちに登録停止メッセージを送り返します。

## 例

次に、「no-ssm-range」という名前のアクセス リストで定義された送信元からの PIM 登録メッセージを制限する例を示します。

```
ciscoasa(config)# pim accept-register list no-ssm-range
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# pim bidir-neighbor-filter

DF 選出に参加できる双方向対応ネイバーを制御するには、インターフェイス コンフィギュレーション モードで **pim bidir-neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

**pim bidir-neighbor-filter** *acl*

**no pim bidir-neighbor-filter** *acl*

## 構文の説明

| | |
|---|---|
| *acl* | アクセス リストの名前または番号を指定します。アクセス リストは、双方向 DF 選出に参加できるネイバーを定義します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。 |

## デフォルト

すべてのルータは双方向対応であると見なされます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

**pim bidir-neighbor-filter** コマンドを使用すると、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。この場合、すべてのルータのスパース モード ドメインへの参加を許可しながら、DF 選出へ参加しなければならないルータを指定します。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

**pim bidir-neighbor-filter** コマンドがイネーブルの場合、ACL で許可されているルータは双方向対応であると見なされます。したがって、次のようにします。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

## 例

次に、10.1.1.1 を PIM 双方向ネイバーにできる例を示します。

```
ciscoasa(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list bidir_test deny any
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidir-neighbor-filter bidir_test
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast boundary** | 管理上有効範囲が設定されたマルチキャスト アドレスに対してマルチキャスト境界を定義します。 |
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# pim bsr-border

ブートストラップ ルータ（BSR）メッセージがインターフェイス経由で送受信されることを防止するには、インターフェイス コンフィギュレーション モードで pim bsr-border コマンドを使用します。

（注） PIM スパース モード（PIM-SM）のドメインの境界インターフェイスには、特にそのインターフェイスによって到達可能な隣接ドメインも PIM-SM を実行している場合、そのドメインとの特定のトラフィックのやりとりを阻止する特別な防止策が必要です。

**pim bsr-border**

**no pim bsr-border**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.5(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドがインターフェイスで設定されている場合、PIM バージョン 2 BSR メッセージはインターフェイス経由で送受信されません。2 つのドメイン間で BSR メッセージが交換されないようにするには、このコマンドで別の PIM ドメインに隣接するインターフェイスを設定します。一方のドメインにあるルータは他方のドメインにあるランデブー ポイント（RP）を選択し、その結果ドメイン間でプロトコルが誤動作したり分離が行われない可能性があるため、BSR メッセージを異なるドメイン間で交換しないでください。

（注） このコマンドはマルチキャスト境界をセットアップしません。PIM ドメイン BSR メッセージ境界のみをセットアップします。

## 例

次に、PIM ドメイン境界となるようにインターフェイスを設定する例を示します。

```
ciscoasa(config)# interface gigabit 0/0
ciscoasa(config-if)# pim bsr-border
ciscoasa(config)# show runn interface gigabitEthernet 0/0
!
interface GigabitEthernet0/0
 nameif outsideA
 security-level 0
 ip address 2.2.2.2 255.255.255.0
 pim bsr-border
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |
| **pim bsr-candidate** | ASA を BSR 候補に設定します。 |

# pim bsr-candidate

ルータがブートストラップ ルータ（BSR）の候補であることをアナウンスするよう設定するには、グローバル コンフィギュレーション モードで **pim bsr-candidate** コマンドを使用します。ブートストラップ ルータの候補としてのこのルータを削除するには、このコマンドの no 形式を使用します。

**pim bsr-candidate** ***interface-name*** **[*hash-mask-length* [*priority*]]**

**no pim bsr-candidate**

## 構文の説明

| | |
|---|---|
| *interface-name* | BSR アドレスが取得されるこのルータでのインターフェイス名。このアドレスは、BSR メッセージで送信されます。 |
| *hash-mask-length* | （任意）PIMv2 ハッシュ機能がコールされる前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）。ハッシュ元が同じであるすべてのグループは、同じランデブー ポイント（RP）に対応します。<br>たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。ハッシュ マスク長により、1 つの RP を複数のグループで使用できるようになります。<br>デフォルトのハッシュ マスク長は 0 です。 |
| *priority* | （任意）BSR（C-BSR）候補のプライオリティ。有効な範囲は 0 ～ 255 です。最高のプライオリティ値を持つ C-BSR が優先されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。<br>デフォルトのプライオリティは 0 です。 |

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

デバイスがハッシュ長およびプライオリティなしで BSR 候補として設定されている場合は、デフォルトのハッシュ長（0）とデフォルトのプライオリティ（0）が前提となります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.5(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドにより、ブートストラップ メッセージは BSR アドレスとして指定されたインターフェイスのアドレスをつけてすべての PIM ネイバーに送信されます。各ネイバーは、以前のブートストラップ メッセージから受信したアドレスと BSR アドレスを比較します(同じインターフェイスで受信される必要はない)。現在のアドレスが同じかまたはより高位のアドレスである場合、現在のアドレスはキャッシュに格納され、ブートストラップ メッセージは転送されます。それ以外の場合は、ブートストラップ メッセージがドロップされます。

この ASA よりもプライオリティが高い(プライオリティが同じ場合は、より高位の IP アドレスを持つ)とされる他の BSR 候補からブートストラップ メッセージを受信するまで、この ASA は BSR のままです。

## 例

次に、「内部」インターフェイスで、30 のハッシュ長と 10 のプライオリティにより、ASA をブートストラップ ルータ(C-BSR)候補として設定する例を示します。

```
ciscoasa(config)# pim bsr-candidate inside 30 10
ciscoasa(config)# sh runn pim
pim bsr-candidate inside 30 10
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |
| **pim bsr-border** | ASA を境界 BSR として設定します。 |

# pim dr-priority

指定ルータ選出に使用される ASA でネイバーのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **pim dr-priority** コマンドを使用します。デフォルトのプライオリティに戻すには、このコマンドの **no** 形式を使用します。

**pim dr-priority** *number*

**no pim dr-priority**

## 構文の説明

| | |
|---|---|
| *number* | 0 ～ 4294967294 の番号。この番号は、指定ルータを決定するときにデバイスのプライオリティを判断するために使用されます。0 を指定すると、ASA は指定ルータになりません。 |

## デフォルト

デフォルト値は 1 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

インターフェイスでプライオリティ値が最大のデバイスが PIM 指定ルータになります。複数のデバイスで指定ルータのプライオリティが同じである場合は、IP アドレスが最大のデバイスが DR になります。デバイスの hello メッセージに DR-Priority Option が含まれていない場合は、プライオリティが最大のデバイスとして扱われ、指定ルータになります。複数のデバイスで hello メッセージにこのオプションが含まれていない場合は、IP アドレスが最大のデバイスが指定ルータになります。

## 例

次に、インターフェイスの DR プライオリティを 5 に設定する例を示します。

```
ciscoasa(config-if)# pim dr-priority 5
```

関連コマンド

| コマンド | 説明 |
| --- | --- |
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# pim hello-interval

PIM hello メッセージの頻度を設定するには、インターフェイス コンフィギュレーション モードで **pim hello-interval** コマンドを使用します。hello-interval をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**pim hello-interval** *seconds*

**no pim hello-interval** [*seconds*]

## 構文の説明

| | |
|---|---|
| *seconds* | ASA が hello メッセージを送信するまでの待機秒数。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 30 秒です。 |

## デフォルト

間隔のデフォルト値は 30 秒です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 例

次に、PIM hello 間隔を 1 分に設定する例を示します。

```
ciscoasa(config-if)# pim hello-interval 60
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# pim join-prune-interval

PIM Join/Prune の間隔を設定するには、インターフェイス コンフィギュレーション モードで **pim join-prune-interval** コマンドを使用します。間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**pim join-prune-interval** *seconds*

**no pim join-prune-interval** [*seconds*]

## 構文の説明

| | |
|---|---|
| *seconds* | ASA が Join/Prune メッセージを送信するまでの待機秒数。有効な値の範囲は、10 ～ 600 秒です。デフォルトは 60 秒です。 |

## デフォルト

デフォルトの間隔は 60 秒です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 例

次に、PIM Join/Prune 間隔を 2 分に設定する例を示します。

```
ciscoasa(config-if)# pim join-prune-interval 120
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# pim neighbor-filter

PIM に参加できるネイバー ルータを制御するには、インターフェイス コンフィギュレーション モードで **pim neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

**pim neighbor-filter** *acl*

**no pim neighbor-filter** *acl*

## 構文の説明

| | |
|---|---|
| *acl* | アクセス リストの名前または番号を指定します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、PIM に参加できるネイバー ルータを定義します。このコマンドがコンフィギュレーションに存在しない場合、制限はありません。

コンフィギュレーションでこのコマンドを使用するには、マルチキャスト ルーティングおよび PIM がイネーブルである必要があります。マルチキャスト ルーティングをディセーブルにすると、このコマンドはコンフィギュレーションから削除されます。

## 例

次に、IP アドレスが 10.1.1.1 であるルータをインターフェイス GigabitEthernet 0/2 で PIM ネイバーにする例を示します。

```
ciscoasa(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list pim_filter deny any
ciscoasa(config)# interface gigabitEthernet0/2
ciscoasa(config-if)# pim neighbor-filter pim_filter
```

関連コマンド

| コマンド | 説明 |
| --- | --- |
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# pim old-register-checksum

古いレジスタ チェックサム方式を使用するランデブー ポイント(RP)での下位互換性を保つには、グローバル コンフィギュレーション モードで **pim old-register-checksum** コマンドを使用します。PIM RFC 準拠レジスタを生成するには、このコマンドの **no** 形式を使用します。

**pim old-register-checksum**

**no pim old-register-checksum**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

ASA は PIM RFC 準拠レジスタを生成します。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

ASA ソフトウェアは、Cisco IOS 方式を使用せずに、PIM ヘッダーにチェックサムのあるレジスタ メッセージとそれに続く 4 バイトのみを受け入れます。つまり、すべての PIM メッセージ タイプについて PIM メッセージ全体を含むレジスタ メッセージを受け入れます。**pim old-register-checksum** コマンドを使用すると、Cisco IOS ソフトウェアと互換性のあるレジスタが生成されます。

## 例

次に、古いチェックサム計算を使用するように ASA を設定する例を示します。

```
ciscoasa(config)# pim old-register-checksum
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# pim rp-address

PIM ランデブー ポイント(RP)のアドレスを使用するには、グローバル コンフィギュレーション モードで **pim rp-address** コマンドを使用します。RP アドレスを削除するには、このコマンドの **no** 形式を使用します。

**pim rp-address** *ip_address* [*acl*] [**bidir**]

**no pim rp-address** *ip_address*

## 構文の説明

| | |
|---|---|
| *acl* | (任意)RP とともに使用されるマルチキャスト グループを定義する標準アクセス リストの名前または番号。このコマンドではホスト ACL を使用しないでください。 |
| **bidir** | (任意)指定したマルチキャスト グループが双方向モードで動作することを指定します。このオプションを指定せずにコマンドを設定した場合、指定したグループは PIM スパース モードで動作します。 |
| *ip_address* | PIM RP になるルータの IP アドレス。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。 |

## デフォルト

PIM RP アドレスは設定されていません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

一般的な PIM スパース モード(PIM-SM)内または双方向ドメイン内にあるすべてのルータは、既知の PIM RP アドレスを認識する必要があります。アドレスは、このコマンドを使用してスタティックに設定されます。

(注) ASA では、Auto-RP をサポートしません。**pim rp-address** コマンドを使用して、RP アドレスを指定する必要があります。

複数のグループにサービスを提供するように単一の RP を設定できます。アクセス リストに指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。アクセス リストを指定しない場合、グループの RP は IP マルチキャスト グループの範囲（224.0.0.0/4）全体に適用されます。

（注） ASA は、実際の双方向コンフィギュレーションとは関係なく、常に双方向機能を PIM hello メッセージ内でアドバタイズします。

## 例

次に、すべてのマルチキャスト グループに対して PIM RP アドレスを 10.0.0.1 に設定する例を示します。

```
ciscoasa(config)# pim rp-address 10.0.0.1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **pim accept-register** | PIM レジスタ メッセージをフィルタリングするように候補 RP を設定します。 |

# pim spt-threshold infinity

常に共有ツリーを使用し、最短パス ツリー(SPT)スイッチオーバーを実行しないようにラスト ホップ ルータの動作を変更するには、グローバル コンフィギュレーション モードで **pim spt-threshold infinity** 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。

**pim spt-threshold infinity** [**group-list** *acl*]

**no pim spt-threshold**

## 構文の説明

| | |
|---|---|
| **group-list** *acl* | (任意)送信元グループはアクセス リストによって制限されていることを示します。*acl* 引数には、標準 ACL を指定する必要があります。拡張 ACL はサポートされません。 |

## デフォルト

ラスト ホップ PIM ルータは、デフォルトで最短パスの送信元に切り替わります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

**group-list** キーワードを使用しない場合、このコマンドはすべてのマルチキャスト グループに適用されます。

## 例

次に、最短パス送信元ツリーに切り替えるのではなく、常に共有ツリーを使用するようにラスト ホップ PIM ルータを設定する例を示します。

```
ciscoasa(config)# pim spt-threshold infinity
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | ASA でマルチキャスト ルーティングをイネーブルにします。 |

# ping

指定したインターフェイスから IP アドレスへの接続をテストするには、特権 EXEC モードで **ping** コマンドを使用します。使用できるパラメータは、通常の ICMP ベースの ping と TCP の ping とで異なります。パラメータで指定できない特性などの値の入力を求める場合は、このコマンドをパラメータなしで入力します。

**ping** [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

**ping tcp** [*if_name*] *host port* [**repeat** *count*] [**timeout** *seconds*] [**source** *host port*]

**ping**

(注) **source** と *port* のオプションは、**tcp** オプションでのみ使用できます。**data**、**size**、および **validate** のオプションは、**tcp** オプションでは使用できません。

## 構文の説明

| | |
|---|---|
| **data** *pattern* | (オプション、ICMP のみ) 16 ビット データ パターン (16 進数形式、0 ～ FFFF) を指定します。デフォルトは 0xabcd です。 |
| *ホスト* | ping の送信先ホストの IPv4 アドレスまたは名前を指定します。ICMP ping では、IPv6 アドレスも指定できます (TCP ping ではサポートされません)。<br>ホスト名を指定する場合が、DNS 名または **name** コマンドで割り当てた名前を使用できます。DNS 名の最大文字数は 128、**name** コマンドで作成した名前の最大文字数は 63 です。DNS 名を使用するように DNS サーバを設定する必要があります。 |
| *if_name* | (オプション) ICMP の場合、*host* がアクセス可能なインターフェイス名を指定します。インターフェイス名は、**nameif** コマンドで設定します。指定しない場合、*host* は IP アドレスに解決され、宛先インターフェイスを決定するためにルーティング テーブルが参照されます。TCP の場合は、送信元からの SYN パケットの送信に使用する入力インターフェイスを指定します。 |
| *port* | (TCP のみ) ping を送信するホストの TCP ポート番号 (1 ～ 65535) を指定します。 |
| **repeat** *count* | (任意) ping 要求を繰り返す回数を指定します。デフォルトは 5 分です。 |
| **size** *bytes* | (オプション、ICMP のみ) データグラム サイズ (バイト単位) を指定します。デフォルトは 100 です。 |
| **source** *host port* | (オプション、TCP のみ) ping の送信元の特定の IP アドレスおよびポートを指定します (特定のポートを指定しない場合は port = 0 を使用します)。 |
| **tcp** | (オプション) TCP での接続をテストします (デフォルトは ICMP です)。TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。TCP ping は同時に複数実行することもできます。 |
| **timeout** *seconds* | (オプション) タイムアウト間隔 (秒数) を指定します。デフォルト値は 2 秒です。 |
| **validate** | (オプション、ICMP のみ) 応答データを検証します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 7.2(1) | DNS 名のサポートが追加されました。 |
| 8.4(1) | **tcp** オプションが追加されました。 |

## 使用上のガイドライン

**ping** コマンドを使用すると、ASA が接続可能かどうか、またはホストがネットワークで使用可能かどうかを判断できます。

通常の ICMP ベースの ping を使用する場合、それらのパケットの送信を禁止する **ICMP** ルールがないことを確認してください（ICMP ルールを使用していなければ、すべての ICMP トラフィックが許可されます）。内部ホストから外部ホストに対して ICMP で ping を送信するには、次のいずれかを実行します。

- エコー応答の場合は、ICMP **access-list** コマンドを使用します。たとえば、すべてのホストに対して ping アクセスを与えるには、**access-list acl_grp permit icmp any any** コマンドを使用し、**access-group** コマンドを使用してテストするインターフェイスに対して **access-list** コマンドをバインドします。
- **inspect icmp** コマンドを使用して ICMP インスペクション エンジンを設定します。たとえば、**inspect icmp** コマンドをグローバル サービス ポリシーの **class default_inspection** クラスに追加すると、内部ホストによって開始されるエコー要求に対して、エコー応答は ASA を通過できます。

TCP ping を使用する場合は、指定したポートでの TCP トラフィックの送受信がアクセス ポリシーで許可されている必要があります。

このコンフィギュレーションは、**ping** コマンドで生成されたメッセージに対して、ASA が応答したり受け入れたりするために必要です。**ping** コマンドの出力は、応答が受け入れられたかどうかを示します。ホストが応答しない場合は、**ping** コマンドを入力すると、次のようなメッセージが表示されます。

```
ciscoasa(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ASA がネットワークに接続していて、トラフィックを送受信していることを確認するには、**show interface** コマンドを使用します。指定した *if_name* の名前は、ping の送信元アドレスとして使用されます。

また、**ping** をパラメータなしで入力して、拡張された ping を実行することもできます。この場合、キーワードとして指定できない一部の特性などのパラメータの入力が求められます。

## 例

次に、他の IP アドレスが ASA から認識できるかどうかを判断する例を示します。

```
ciscoasa# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、DNS 名を使用してホストを指定する例を示します。

```
ciscoasa# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、拡張された ping を使用する例を示します。

```
ciscoasa# ping
TCP [n]:
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、**ping tcp** コマンドの例を示します。

```
ciscoasa# ping
TCP [n]: yes
Interface: dmz
Target IP address: 10.0.0.1
Target IP port: 21
Specify source? [n]: y
Source IP address: 192.168.2.7
Source IP port: [0] 465
Repeat count: [5]
Timeout in seconds: [2] 5
Type escape sequence to abort.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 192.168.2.7 starting port 465, timeout is 5 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ciscoasa# ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms


ciscoasa# ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
```

```
ciscoasa(config)# ping tcp www.example.com 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 74.125.19.103 port 80
from 171.63.230.107, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/4 ms

ciscoasa# ping tcp 192.168.1.7 23 source 192.168.2.7 24966
Type escape sequence to abort.
Source port 24966 in use! Using port 24967 instead.
Sending 5 TCP SYN requests to 192.168.1.7 port 23
from 192.168.2.7 starting port 24967, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **icmp** | インターフェイスが終端となる ICMP トラフィックのアクセス ルールを設定します。 |
| **show interface** | VLAN コンフィギュレーションの情報を表示します。 |