CHAPTER 21

nac policy コマンド～ override-svc-download コマンド

nac-policy

シスコ Network Admission Control（NAC; ネットワーク アドミッション コントロール）ポリシーを作成またはアクセスし、そのタイプを指定するには、グローバル コンフィギュレーション モードで **nac-policy** コマンドを使用します。NAC ポリシーをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

nac-policy *nac-policy-name* **nac-framework**

[**no**] **nac-policy** *nac-policy-name* **nac-framework**

構文の説明

nac-policy-name	NAC ポリシーの名前。最大 64 文字で NAC ポリシーの名前を指定します。**show running-config nac-policy** コマンドは、セキュリティ アプライアンスにすでに存在する各 NAC ポリシーの名前およびコンフィギュレーションを表示します。
nac-framework	NAC フレームワークを使用して、リモート ホストのネットワーク アクセス ポリシーを提供することを指定します。セキュリティ アプライアンスの NAC フレームワーク サービスを提供するには、シスコ アクセス コントロール サーバがネットワークに存在している必要があります。 このタイプを指定した場合、プロンプトは現在のモードが設定 nac ポリシー nac フレームワーク コンフィギュレーション モードであることを示します。このモードでは、NAC フレームワーク ポリシーを設定できます。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

グループ ポリシーに割り当てられる NAC アプライアンスごとにこのコマンドを一度使用します。次に、**nac-settings** コマンドを使用して、該当する各グループ ポリシーに NAC ポリシーを割り当てます。IPSec または Cisco AnyConnect VPN トンネルのセットアップ時に、セキュリティ アプライアンスは使用中のグループ ポリシーに関連付けられた NAC ポリシーを適用します。

NAC ポリシーが 1 つ以上のグループ ポリシーにすでに割り当てられている場合、**no nac-policy** *name* コマンドではその NAC ポリシーを削除できません。

例

次のコマンドでは、NAC フレームワーク ポリシーを nac-framework1 という名前で作成し、そのポリシーにアクセスしています。

```
hostname(config)# nac-policy nac-framework1 nac-framework
hostname(config-nac-policy-nac-framework)
```

次のコマンドでは、nac-framework1 という名前の NAC フレームワーク ポリシーを削除しています。

```
hostname(config)# no nac-policy nac-framework1
hostname(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
show running-config nac-policy	セキュリティ アプライアンス上の各 NAC ポリシーのコンフィギュレーションを表示します。
show nac-policy	セキュリティ アプライアンスでの NAC ポリシー使用状況の統計情報を表示します。
clear nac-policy	NAC ポリシー使用状況の統計情報をリセットします。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
clear configure nac-policy	グループ ポリシーに割り当てられているものを除き、すべての NAC ポリシーを実行コンフィギュレーションから削除します。

nac-settings

NAC ポリシーをグループ ポリシーに割り当てるには、次のようにグループ ポリシー コンフィギュレーション モードで **nac-settings** コマンドを使用します。

nac-settings {**value** *nac-policy-name* | **none**}

[**no**] **nac-settings** {**value** *nac-policy-name* | **none**}

構文の説明

nac-policy-name	グループ ポリシーに割り当てられる NAC ポリシー。名前を付ける NAC ポリシーは、セキュリティ アプライアンスのコンフィギュレーションに存在している必要があります。**show running-config nac-policy** コマンドは、各 NAC ポリシーの名前および設定を表示します。
none	グループ ポリシーから *nac-policy-name* を削除し、このグループ ポリシーに関して NAC ポリシーの使用をディセーブルにします。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承しません。
value	名前を付ける NAC ポリシーをグループ ポリシーに割り当てます。

デフォルト

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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

nac-policy コマンドを使用して NAC ポリシーの名前およびタイプを指定してから、このコマンドを使用してそれをグループ ポリシーに割り当てます。

show running-config nac-policy コマンドは、各 NAC ポリシーの名前および設定を表示します。

NAC ポリシーをグループ ポリシーに割り当てると、セキュリティ アプライアンスはそのグループ ポリシーの NAC を自動的にイネーブルにします。

例

次のコマンドでは、グループ ポリシーから *nac-policy-name* を削除しています。グループ ポリシーは、デフォルトのグループ ポリシーから *nac-settings* 値を継承します。

```
hostname(config-group-policy)# no nac-settings
hostname(config-group-policy)
```

次のコマンドでは、グループ ポリシーから *nac-policy-name* を削除し、このグループ ポリシーに関して NAC ポリシーの使用をディセーブルにしています。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承しません。

```
hostname(config-group-policy)# nac-settings none
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
show running-config nac-policy	セキュリティ アプライアンス上の各 NAC ポリシーのコンフィギュレーションを表示します。
show nac-policy	セキュリティ アプライアンスでの NAC ポリシー使用状況の統計情報を表示します。
show vpn-session_summary.db	IPSec セッション、WebVPN セッション、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

name

IP アドレスに名前を関連付けるには、グローバル コンフィギュレーション モードで **name** コマンドを使用します。テキスト名の使用はディセーブルにするが、コンフィギュレーションからは削除しない場合は、このコマンドの **no** 形式を使用します。

name *ip_address name* [description *text*]]

no name *ip_address* **[***name* [description *text*]**]**

構文の説明

description	（任意）IP アドレス名の説明を指定します。
ip_address	名前を付けるホストの IP アドレスを指定します。
name	IP アドレスに割り当てられる名前を指定します。使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ダッシュ、およびアンダースコアです。*name* は、63 文字以下である必要があります。また、*name* は数値で開始できません。
text	説明のテキストを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.0(4)	このコマンドは、任意の説明を含めることができるように拡張されました。

使用上のガイドライン

名前と IP アドレスとの関連付けをイネーブルにするには、**names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。

name コマンドを使用する前に **names** コマンドを使用する必要があります。**name** コマンドは、**names** コマンドを使用した直後、かつ **write memory** コマンドよりも前に使用します。

name コマンドを使用すると、テキスト名でホストを識別し、テキスト ストリングを IP アドレスにマッピングします。**no name** コマンドを使用すると、テキスト名の使用をディセーブルにできます。ただし、コンフィギュレーションからはテキスト名は削除されません。コンフィギュレーションから名前のリストをクリアするには、**clear configure name** コマンドを使用します。

name 値の表示をディセーブルにするには、**no names** コマンドを使用します。

name コマンドと **names** コマンドは両方ともコンフィギュレーションに保存されます。

name コマンドは、ネットワーク マスクへの名前の割り当てをサポートしません。たとえば、次のコマンドは拒否されます。

```
hostname(config)# name 255.255.255.0 class-C-mask
```

（注） マスクを必要とするいずれのコマンドも、受け入れ可能なネットワーク マスクとして名前を処理できません。

例

次に、**names** コマンドを使用して、**name** コマンドの使用をイネーブルにする例を示します。**name** コマンドは、192.168.42.3 の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用します。IP アドレスをネットワーク インターフェイスに割り当てるときに、**ip address** コマンドでこれらの名前を使用できます。**no names** コマンドは、**name** コマンド値の表示をディセーブルにします。後で **names** コマンドを使用すると、**name** コマンド値が再度表示されるようになります。

```
hostname(config)# names
hostname(config)# name 192.168.42.3 sa_inside
hostname(config)# name 209.165.201.3 sa_outside

hostname(config-if)# ip address inside sa_inside 255.255.255.0
hostname(config-if)# ip address outside sa_outside 255.255.255.224

hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224

hostname(config)# no names
hostname(config)# show ip address
System IP Addresses:
    inside ip address 192.168.42.3 mask 255.255.255.0
    outside ip address 209.165.201.3 mask 255.255.255.224

hostname(config)# names
hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前のリストをクリアします。
names	名前と IP アドレスの関連付けをイネーブルにします。
show running-config name	IP アドレスに関連付けられた名前を表示します。

nameif

インターフェイスの名前を指定するには、インターフェイス コンフィギュレーション モードで **nameif** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。インターフェイス名はインターフェイス タイプおよび ID（gigabitethernet0/1 など）ではなくセキュリティ アプライアンスのすべてのコンフィギュレーション コマンドで使用されるため、インターフェイス名がないとトラフィックはインターフェイスを通過できません。

nameif *name*

no nameif

構文の説明

name	最大 48 文字で名前を設定します。名前は大文字と小文字が区別されません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モード コマンドに変更されました。

使用上のガイドライン

サブインターフェイスの場合、**nameif** コマンドを入力する前に、**vlan** コマンドで VLAN を割り当てる必要があります。

名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

例

次に、2 つのインターフェイスにそれぞれ「inside」と「outside」という名前を設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/0
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
```

```
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に対するすべての変換をリセットして、その結果として接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
security-level	インターフェイスのセキュリティ レベルを設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

names

名前と IP アドレスの関連付け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 **names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。**name** 値の表示をディセーブルにするには、**no names** コマンドを使用します。

names

no names

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

names コマンドは、**name** コマンドで設定した名前と IP アドレスの関連付けをイネーブルにするために使用します。**name** または **names** コマンドを入力する順序は、重要ではありません。

例

次に、名前と IP アドレスの関連付けをイネーブルにする例を示します。

```
hostname(config)# names
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前のリストをクリアします。
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられた名前のリストを表示します。
show running-config names	IP アドレスと名前の変換を表示します。

name-separator

電子メール、VPN ユーザ名、パスワード間のデリミタとなる文字を指定するには、適用可能な電子メール プロキシ モードで **name-separator** コマンドを使用します。デフォルトの「:」に戻すには、このコマンドの **no** 形式を使用します。

name-separator [*symbol*]

no name-separator

構文の説明

symbol	（任意）電子メール、VPN ユーザ名、パスワードを区切る文字。選択肢は「@」（アット マーク）、「|」（パイプ）、「:（コロン）」、「|（ハッシュ）」、「,（カンマ）」、「;」（セミコロン）です。

デフォルト

デフォルトは「:」（コロン）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

名前の区切り文字には、サーバの区切り文字とは異なる文字を使用する必要があります。

例

次に、番号記号（#）を POP3S の名前区切り文字として設定する例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# name-separator #
```

関連コマンド

コマンド	説明
server-separator	電子メールとサーバ名を区切ります。

name-server

1 つ以上の DNS サーバを識別するには、DNS サーバ グループ コンフィギュレーション モードで **name-server** コマンドを使用します。1 つ以上のサーバを削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、DNS を使用して、SSL VPN コンフィギュレーションまたは証明書設定のサーバ名を解決します（サポートされているコマンドのリストについては、「使用上のガイドライン」を参照してください）。サーバ名（AAA など）を定義するその他の機能は、DNS 解決をサポートしていません。IP アドレスを入力するか、または **name** コマンドを使用して名前を IP アドレスに手動で解決する必要があります。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

no name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

構文の説明

ip_address	DNS サーバの IP アドレスを指定します。最大 6 つのアドレスを個別のコマンドとして指定するか、便宜上最大 6 つのアドレスをスペースで区切って 1 つのコマンドで指定できます。1 つのコマンドに複数のサーバを入力した場合、セキュリティ アプライアンスはそれぞれのサーバを個別のコマンドとしてコンフィギュレーションに保存します。セキュリティ アプライアンスでは、応答を受信するまで各 DNS サーバを順に試します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

DNS ルックアップをイネーブルにするには、DNS サーバ グループ コンフィギュレーション モードで **domain-name** コマンドを設定します。DNS ルックアップをイネーブルにしないと、DNS サーバは使用されません。

DNS 解決をサポートする SSL VPN コマンドには、次のものがあります。

- **server（pop3s）**
- **server（imap4s）**
- **server（smtps）**
- **port-forward**

- **url-list**

DNS 解決をサポートする証明書のコマンドには、次のものがあります。

- **enrollment url**
- **url**

name コマンドを使用して、名前および IP アドレスを手動で入力できます。

例

次に、3 つの DNS サーバをグループ「dnsgroup1」に追加する例を示します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

セキュリティ アプライアンスは、次のように、別々のコマンドとしてコンフィギュレーションを保存します。

```
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
```

さらに 2 つのサーバを追加するには、それらを 1 つのコマンドとして入力します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

DNS サーバ グループ コンフィギュレーションを確認するには、グローバル コンフィギュレーション モードで **show running-config dns** コマンドを入力します。

```
hostname(config)# show running-config dns
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
name-server 10.5.1.1
name-server 10.8.3.8
...
```

また、それらを 2 つの個別のコマンドとして入力することもできます。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.5.1.1
hostname(config)# name-server 10.8.3.8
```

複数のサーバを削除するには、次のようにそれらのサーバを複数のコマンドまたは 1 つのコマンドとして入力します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# no name-server 10.5.1.1 10.8.3.8
```

関連コマンド

コマンド	説明
domain-name	デフォルトのドメイン名を設定します。
retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show running-config dns server-group	既存の DNS サーバ グループ コンフィギュレーションのうちの 1 つまたはすべてを表示します。

nat

あるインターフェイス上のアドレスのうち、別のインターフェイス上のマッピング先のアドレスに変換されるアドレスを識別するには、グローバル コンフィギュレーション モードで **nat** コマンドを使用します。このコマンドは、プールされたマッピング先のアドレスのいずれかにアドレスが変換されるダイナミック NAT または PAT を設定します。**nat** コマンドを削除するには、このコマンドの **no** 形式を使用します。

通常のダイナミック NAT の場合：

nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

no nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

ポリシー ダイナミック NAT および NAT 免除の場合：

nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

no nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

構文の説明

access-list *access_list_name*	ポリシー NAT とも呼ばれる拡張アクセス リストを使用して、ローカル アドレスおよび宛先アドレスを識別します。**access-list** コマンドを使用して、アクセス リストを作成します。**eq** 演算子を使用して、アクセス リストに任意でローカル ポートおよび宛先ポートを指定できます。NAT ID が **0** の場合、アクセス リストでは NAT が免除されるアドレスが指定されます。NAT 免除は、ポリシー NAT と同じではありません。NAT 免除では、たとえば、ポート アドレスは指定できません。 **（注）** **show access-list** コマンドによって表示されるアクセス リストのヒット カウントは、NAT 免除アクセス リストでは増加しません。
dns	（任意）このコマンドに一致する DNS 応答で A レコード（アドレス レコード）を書き換えます。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へリライトされます。 DNS サーバにエントリがあるホストのアドレスが NAT ステートメントに含まれ、その DNS サーバがクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストにそれぞれ異なるアドレスを必要とします。つまり、一方はグローバル アドレスを必要とし、もう一方はローカル アドレスを必要とします。変換されたホストは、クライアントまたは DNS サーバと同じインターフェイスに存在する必要があります。一般に、他のインターフェイスからのアクセスを許可する必要があるホストは static 変換を使用するため、**static** コマンドではこのオプションの方が使用される可能性が高くなります。

emb_limit	（任意）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。 NAT 免除（**nat 0 access-list**）はサポートされていません。この引数は CLI で入力できますが、コンフィギュレーションには保存されません。
mask	（任意）実アドレスのサブネット マスクを指定します。マスクを入力しないと、IP アドレス クラスのデフォルト マスクが使用されます。
nat_id	NAT ID の整数を指定します。通常の NAT の場合、この整数の範囲は 1 ～ 2147483647 となります。ポリシー NAT（nat id access-list）の場合、整数の範囲は 1 ～ 65535 となります。 アイデンティティ NAT（**nat 0**）および NAT 免除（**nat 0 access-list**）は、NAT ID に **0** を使用します。 この ID は、グローバル プールを *real_ip* に関連付けるために、**global** コマンドで参照されます。
norandomseq	（任意）TCP ISN のランダム化保護をディセーブルにします。NAT 免除（**nat 0 access-list**）はサポートされていません。この引数は CLI で入力できますが、コンフィギュレーションには保存されません。 それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。 保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。 TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。 • 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。 • セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。 • セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
outside	（任意）このインターフェイスが **global** ステートメントの照合によって識別したインターフェイスよりも低いセキュリティ レベルにある場合、**outside** を入力する必要があります。この機能は、外部 NAT または双方向 NAT と呼ばれます。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実アドレスを指定します。**0.0.0.0**（または短縮形 **0**）を使用して、すべてのアドレスを指定できます。

tcp *tcp_max_conns*	（任意）ローカル ホストに許可する同時 TCP 接続の最大数を指定します（**local-host** コマンドを参照）。デフォルトは 0 です。接続数の制限がないことを意味します （アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 接続制限を設定するために推奨される方法は、ポリシー マップの中でクラスに接続制限を設定して、モジュラ ポリシー フレームワークを使用することです。 NAT 免除（**nat 0 access-list**）はサポートされていません。この引数は CLI で入力できますが、コンフィギュレーションには保存されません。
udp *udp_max_conns*	（任意）ローカル ホストに許可する同時 UDP 接続の最大数を指定します（**local-host** コマンドを参照）。デフォルトは 0 です。接続数の制限がないことを意味します （アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 接続制限を設定するために推奨される方法は、ポリシー マップの中でクラスに接続制限を設定して、モジュラ ポリシー フレームワークを使用することです。 NAT 免除（**nat 0 access-list**）はサポートされていません。この引数は CLI で入力できますが、コンフィギュレーションには保存されません。

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	NAT は、トランスペアレント ファイアウォール モードでサポートされるようになりました。

使用上のガイドライン

ダイナミック NAT と PAT の場合、最初に **nat** コマンドを設定し、変換する所定のインターフェイスの実アドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマッピング アドレスを指定します（PAT の場合、このアドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てられた番号である NAT ID の比較によって、1 つの **global** コマンドと一致します。

NAT コントロール

セキュリティ アプライアンスは、NAT ルールがトラフィックに一致すると、アドレスを変換します。NAT ルールが一致しなかった場合、パケットの処理が続行されます。例外は、**nat-control** コマンドを使用して NAT コントロールをイネーブルにした場合です。NAT コントロールをイネーブルにした場合、セキュリティの高いインターフェイス（inside）からセキュリティの低いインターフェイス（outside）に移動するパケットは NAT ルールに一致する必要があり、一致しないとそのパケットの処理は停止します。セキュリティ レベルが同じインターフェイス間では、NAT コントロールをイネーブルにした場合でも、NAT は必要ありません。必要に応じて任意で NAT を設定できます。**nat-control** コマンドは、旧バージョンのセキュリティ アプライアンスで定義された NAT コンフィギュレーションに対して使用します。NAT ルールが存在しないことに基づくのではなく、アクセス コントロールにアクセス ルールを使用して、セキュリティ アプライアンスを通過するトラフィックを阻止することがベスト プラクティスです。

ダイナミック NAT の概要

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピング プールには、実アドレス グループよりも少ない数のアドレスを含めることができます。変換対象のホストが宛先ネットワークにアクセスすると、セキュリティ アプライアンスは、マッピング プールから IP アドレスをそのホストに割り当てます。この変換は、実ホストが接続を開始するときにだけ追加されます。変換は、接続が維持されている間のみ機能します。変換がタイムアウトすると、ユーザが同じ IP アドレスを保持することはありません（**timeout xlate** コマンドを参照）。このため、宛先ネットワーク上のユーザはダイナミック NAT（または PAT）を使用するホストへの接続を（接続がアクセス リストで許容されていても）確実には開始できません。セキュリティ アプライアンスは、実ホスト アドレスへの直接接続を拒否します。ホストへの信頼性の高いアクセスについては、**static** コマンドを参照してください。

ダイナミック NAT の長所と短所

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  この事象が発生した場合には、PAT を使用します。PAT では、単一アドレスのポートを使用して 64,000 を超える変換を処理できるためです。

- マッピング プールでは、ルーティング可能なアドレスを多数使用する必要があります。インターネットのように宛先ネットワークで登録済みアドレスが必要になる場合は、使用可能なアドレスが不足することがあります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は GRE バージョン 0 などポートが過負荷にならない IP プロトコルでは機能しません。また、データ ストリームと制御パスが別々のポートにあり、オープン規格でないアプリケーション（一部のマルチメディア アプリケーション）でも機能しません。

ダイナミック PAT の概要

PAT は、複数の実アドレスを単一のマッピング IP アドレスに変換します。特に、セキュリティ アプライアンスは実アドレスと送信元ポート（実ソケット）をマッピング先のアドレスと 1024 より上の一意のポート（マッピング ソケット）に変換します。接続ごとに送信元ポートが異なるため、それぞれの接続で個別に変換を行う必要があります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

接続の有効期限が切れると、ポート変換も 30 秒間の非アクティブ状態の後に有効期限切れになります。このタイムアウトは変更できません。

PAT では単一のマッピング先のアドレスを使用するため、ルーティング可能なアドレスの使用を抑えることができます。さらに、セキュリティ アプライアンス インターフェイスの IP アドレスを PAT アドレスとして使用できます。PAT は、データ ストリームが制御パスとは別のものであるマルチメディア アプリケーションでは機能しません。

（注）　変換の実施中、リモート ホストから、変換されたホストへの接続を開始できます（その接続がアクセス リストで許可されている場合）。アドレス（実アドレスとマッピング先のアドレスの両方）は予測できないため、ホストへの接続が確立される可能性はほとんどありません。ただし、この場合、アクセス リストのセキュリティを利用できます。

NAT のバイパス

NAT コントロールをイネーブルにした場合、内部ホストは、外部ホストにアクセスするときに NAT ルールに一致する必要があります。一部のホストに対して NAT を実行しない場合は、それらのホストに関する NAT をバイパスします（あるいは、NAT コントロールをディセーブルにします）。NAT をサポートしないアプリケーションを使用している場合などには、NAT をバイパスすることを推奨します。**static** コマンドを使用すると、NAT や次のいずれかのオプションをバイパスできます。

- アイデンティティ NAT（**nat 0** コマンド）：アイデンティティ NAT（ダイナミック NAT に似ています）を設定するときは、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続にアイデンティティ NAT を使用する必要があります。このため、インターフェイス A にアクセスするときには実アドレスに対して通常の変換の実行を選択できませんが、インターフェイス B にアクセスするときにはアイデンティティ NAT を使用できます。一方、通常のダイナミック NAT では、アドレス変換を実施する特定のインターフェイスを指定できます。アイデンティティ NAT を使用する実アドレスが、アクセス リストに従って使用できるすべてのネットワークでルーティング可能であることを確認します。

  アイデンティティ NAT の場合、マッピング先のアドレスは実アドレスと同じですが、外部から内部への接続を（インターフェイスのアクセス リストで許可されていても）開始できません。この機能には、スタティックなアイデンティティ NAT または NAT 免除を使用してください。

- NAT 免除（**nat 0 access-list** コマンド）：NAT 免除を使用すると、変換後のホストとリモート ホストの両方が接続を開始できます。アイデンティティ NAT と同様に、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では、変換する実アドレスを判別するときに実アドレスおよび宛先アドレスを指定できるため（ポリシー NAT に似ています）、NAT 免除を使用する方が制御の柔軟性が増します。その反面、ポリシー NAT と異なり、NAT 免除ではアクセス リストのポートが考慮されません。また、NAT 免除は **tcp** キーワードや **udp** キーワードなどの接続設定をサポートしません。

ポリシー NAT

ポリシー NAT を使用すると、拡張アクセス リストに送信元アドレスおよび宛先アドレスを指定することにより、アドレス変換の実アドレスを識別できます。任意で送信元ポートおよび宛先ポートを指定することもできます。通常の NAT でのみ、実アドレスを考慮できます。たとえば、実アドレスがサーバ A にアクセスするときにはその実アドレスをマッピング先のアドレス A に変換できますが、実アドレスがサーバ B にアクセスするときにはその実アドレスをマッピング先のアドレス B に変換できます。

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

（注）　NAT 免除以外のすべてのタイプの NAT が、ポリシー NAT をサポートします。NAT 免除はアクセス リストを使用して実アドレスを識別しますが、ポリシー NAT とは異なり、ポートが考慮されません。ポリシー NAT をサポートする**スタティックな**アイデンティティ NAT を使用すると、NAT 免除と同じ結果を得ることができます。

モジュラ ポリシー フレームワーク を使用した接続設定

モジュラ ポリシー フレームワーク を使用することによっても、接続制限を設定できます（ただし、初期接続制限は設定できません）。詳細については、**set connection** コマンドを参照してください。初期接続制限を設定するには、NAT を使用する必要があります。両方の方法を使用して同じトラフィックにこれらの設定を行う場合は、セキュリティ アプライアンスは低い方の制限を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

変換セッションのクリア

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするまで待たずに新しい NAT 情報を使用するために、**clear xlate** コマンドを使用して変換テーブルをクリアできます。ただし、変換テーブルをクリアすると、現在の接続がすべて切断されます。

例

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスと共に指定するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
```

```
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
clear configure nat	NAT コンフィギュレーションを削除します。
global	グローバル アドレスのプールからエントリを作成します。
interface	インターフェイスを作成および設定します。
show running-config nat	ネットワークに関連付けられているグローバル IP アドレスのプールを表示します。

nat（vpn ロードバランシング）

このデバイスの IP アドレスを NAT でどの IP アドレスに変換するかを設定するには、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 **nat** コマンドを使用します。この NAT 変換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。

nat *ip-address*

no nat [*ip-adddress*]

構文の説明

ip-address	この NAT でこのデバイスの IP アドレスの変換先となる IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**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。

このコマンドの **no nat** 形式で任意の *ip-address* 値を指定する場合は、IP アドレスが実行コンフィギュレーションの既存の NAT IP アドレスに一致する必要があります。

例

次に、nat 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。この **nat** コマンドでは、NAT で変換するアドレスを 192.168.10.10 に設定しています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
```

```
hostname(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。

nat-control

NAT コントロールを有効にするには、グローバル コンフィギュレーション モードで **nat-control** コマンドを使用します。内部ホストが外部にアクセスする場合は、NAT コントロールに内部ホストの NAT が必要になります。NAT コントロール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。

nat-control

no nat-control

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

NAT コントロールは、デフォルトではディセーブルです（**no nat-control** コマンド）。ただし、旧バージョンのソフトウェアからアップグレードした場合には、システムで NAT コントロールがイネーブルになっていることがあります。旧バージョンによってはイネーブルがデフォルトであったためです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.3.(1)	NAT は、トランスペアレント ファイアウォール モードでサポートされるようになりました。

使用上のガイドライン

NAT コントロールをイネーブルにした場合、内部インターフェイスから外部インターフェイスに移動するパケットは NAT ルールに一致する必要があります。内部ネットワーク上のホストが外部ネットワーク上のホストにアクセスする場合には、内部ホストのアドレスを変換するように NAT を設定する必要があります。

nat-control コマンドは、旧バージョンのセキュリティ アプライアンスで定義された NAT コンフィギュレーションに対して使用します。NAT ルールが存在しないことに基づくのではなく、アクセス コントロールにアクセス ルールを使用して、セキュリティ アプライアンスを通過するトラフィックを阻止することがベスト プラクティスです。

セキュリティ レベルが同じインターフェイス同士で通信する場合には、NAT を使用する必要はありません。ただし、NAT コントロールをイネーブルにして同じセキュリティのインターフェイスにダイナミック NAT または PAT を設定した場合は、インターフェイスから同じセキュリティのインターフェイスまたは外部インターフェイスに移動するすべてのトラフィックが、NAT ルールに一致する必要があります。

同様に、NAT コントロールで外部ダイナミック NAT または PAT をイネーブルにした場合は、内部インターフェイスにアクセスするときには、すべての外部トラフィックが NAT ルールに一致する必要があります。

NAT コントロールをイネーブルにしたスタティック NAT では、これらの制限がありません。

デフォルトでは、NAT コントロールはディセーブルであるため、NAT の実行を選択しない限り、どのネットワークでも NAT を実行する必要はありません。

（注） マルチ コンテキスト モードでは、パケット分類子が NAT コンフィギュレーションを利用してパケットをコンテキストに割り当てる場合があります。NAT コントロールがディセーブルであるために NAT を実行しない場合は、ネットワーク設定の変更が必要になることがあります。

NAT コントロールのセキュリティは強化するものの、場合によっては内部アドレスを変換しないようにする場合は、その内部アドレスに NAT 免除（**nat 0 access-list**）またはアイデンティティ NAT（**nat 0** または **static**）ルールを適用できます。

no-nat control コマンドで NAT コントロールがディセーブルにされており、インターフェイスに NAT と global コマンドのペアが設定されている場合、実 IP アドレスから他のインターフェイスに移動するには、**nat 0 access-list** コマンドでその宛先を定義する必要があります。

たとえば、次の NAT は外部ネットワークに移動するときに実施したものです。

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 209.165.201.2
```

上記のコンフィギュレーションでは、内部ネットワークであらゆるデータを捕捉するため、内部アドレスが DMZ に移動するときにその内部アドレスを変換しない場合は、次の例に示すように、NAT 免除に関してトラフィックを照合する必要があります。

```
access-list EXEMPT extended permit ip any 192.168.1.0 255.255.255.0
access-list EXEMPT remark This matches any traffic going to DMZ1
access-list EXEMPT extended permit ip any 10.1.1.0 255.255.255.0
access-list EXEMPT remark This matches any traffic going to DMZ2
nat (inside) 0 access-list EXEMPT
```

この他に、すべてのインターフェイスで NAT 変換を実行することもできます。

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 209.165.201.2
global (dmz1) 1 192.168.1.230
global (dmz2) 1 10.1.1.230
```

例

次に、NAT コントロールをイネーブルにする例を示します。

```
hostname(config)# nat-control
```

関連コマンド

コマンド	説明
nat	インターフェイス上で、別のインターフェイス上のマッピング先のアドレスに変換されるアドレスを定義します。
show running-config nat-control	NAT コンフィギュレーション要件を表示します。
static	実アドレスをマッピング先のアドレスに変換します。

nat-rewrite

DNS 応答の A レコードに組み込まれている IP アドレスの NAT リライトをイネーブルにするには、パラメータ コンフィギュレーション モードで **nat-rewrite** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

nat-rewrite

no nat-rewrite

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

NAT リライトは、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定していれば、イネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションに **no nat-rewrite** を明示的に指定する必要があります。**inspect dns** が設定されていない場合、NAT リライトは実行されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

この機能は、DNS 応答の A タイプの Resource Record（RR; リソース レコード）の NAT 変換を実行します。

例

次に、DNS インスペクション ポリシー マップで NAT リライトをイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# nat-rewrite
```

関連コマンド

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

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

nbns-server（トンネル グループ webvpn 属性モード）

NBNS サーバを設定するには、トンネル グループ webvpn コンフィギュレーション モードで **nbns-server** コマンドを使用します。コンフィギュレーションから NBNS サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NBNS サーバに照会します。WebVPN では、リモート システム上のファイルへのアクセスまたはファイルの共有に NetBIOS が必要です。

nbns-server {*ipaddr* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

構文の説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	これは WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバへのクエリーを再試行する回数を指定します。セキュリティ アプライアンスは、エラー メッセージを送信するまでに、ここに指定する回数、サーバのリストを循環して使用します。デフォルト値は 2 で、指定できる範囲は 1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	NBNS サーバが 1 つだけ存在する場合は同じサーバに、複数存在する場合は別のサーバに、セキュリティ アプライアンスがクエリーを再送信するまでに待機する時間を指定します。デフォルトのタイムアウトは 2 秒で、指定できる範囲は 1 ～ 30 秒です。

デフォルト

NBNS サーバは、デフォルトでは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn モードからトンネル グループ webvpn コンフィギュレーション モードに移行しました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn 属性コンフィギュレーション モードの同等のコマンドに変換されます。

サーバ エントリは最大 3 つです。冗長性のために、設定する最初のサーバはプライマリ サーバで、その他のサーバはバックアップです。

no オプションを使用して、コンフィギュレーションから一致するエントリを削除します。

例

次に、NBNS サーバでトンネル グループ「test」を設定する例を示します。NBNS サーバはマスター ブラウザであり、IP アドレスを 10.10.10.19、タイムアウト値を 10 秒、および再試行回数を 8 としています。また、IP アドレス 10.10.10.24、タイムアウト値 15 秒、再試行回数 8 回の NBNS WINS サーバを設定する例も示します。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	指定したトンネル グループの WebVPN 属性を指定します。

nbns-server（webvpn モード）

NBNS サーバを設定するには、トンネル グループ webvpn コンフィギュレーション モードで **nbns-server** コマンドを使用します。コンフィギュレーションから NBNS サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NBNS サーバに照会します。WebVPN では、リモート システム上のファイルへのアクセスまたはファイルの共有に NetBIOS が必要です。

nbns-server {*ipaddr* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

構文の説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	これは WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバへのクエリーを再試行する回数を指定します。セキュリティ アプライアンスは、エラー メッセージを送信するまでに、ここに指定する回数、サーバのリストを循環して使用します。デフォルト値は 2 で、指定できる範囲は 1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	NBNS サーバが 1 つだけ存在する場合は同じサーバに、複数存在する場合は別のサーバに、セキュリティ アプライアンスがクエリーを再送信するまでに待機する時間を指定します。デフォルトのタイムアウトは 2 秒で、指定できる範囲は 1 ～ 30 秒です。

デフォルト

NBNS サーバは、デフォルトでは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn モードからトンネル グループ webvpn コンフィギュレーション モードに移行しました。

使用上のガイドライン

このコマンドは、webvpn コンフィギュレーション モードでは廃止されました。トンネル グループ webvpn 属性コンフィギュレーション モードの nbns-server コマンドに置き換えられました。リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn 属性モードの同等のコマンドに変換されます。

サーバ エントリは最大 3 つです。冗長性のために、設定する最初のサーバはプライマリ サーバで、その他のサーバはバックアップです。

no オプションを使用して、コンフィギュレーションから一致するエントリを削除します。

例

次に、NBNS サーバを設定する例を示します。NBNS サーバはマスター ブラウザであり、IP アドレスを 10.10.10.19、タイムアウト値を 10 秒、および再試行回数を 8 としています。また、IP アドレス 10.10.10.24、タイムアウト値 15 秒、再試行回数 8 回の NBNS WINS サーバを設定する例も示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
```

neighbor

ポイントツーポイントの非ブロードキャスト ネットワークにスタティック ネイバーを定義するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。コンフィギュレーションからスタティックに定義されたネイバーを削除するには、このコマンドの **no** 形式を使用します。**neighbor** コマンドは、VPN トンネル経由で OSPF ルートをアドバタイズするために使用されます。

neighbor *ip_address* [**interface** *name*]

no neighbor *ip_address* [**interface** *name*]

構文の説明

interface *name*	（任意）**nameif** コマンドで指定されたインターフェイス名。ネイバーにはこのインターフェイス経由で到達できます。
ip_address	隣接ルータの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

既知の非ブロードキャスト ネットワーク ネイバーごとにネイバー エントリを 1 つ含める必要があります。ネイバー アドレスは、インターフェイスのプライマリ アドレスに存在する必要があります。

ネイバーがシステムに直接接続されたいずれかのインターフェイスと同じネットワークにないときには、**interface** オプションを指定する必要があります。また、ネイバーに到達するには、スタティック ルートを作成する必要があります。

例

次に、アドレス 192.168.1.1 で隣接ルータを定義する例を示します。

```
hostname(config-router)# neighbor 192.168.1.1
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

neighbor（EIGRP）

ルーティング情報を交換する EIGRP 隣接ルータを定義するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。ネイバー エントリを削除するには、このコマンドの **no** 形式を使用します。

neighbor *ip_address* **interface** *name*

no neighbor *ip_address* **interface** *name*

構文の説明

interface *name*	**nameif** コマンドで指定されたインターフェイス名。ネイバーにはこのインターフェイス経由で到達できます。
ip_address	隣接ルータの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

複数のネイバー ステートメントを使用して、特定の EIGRP ネイバーでピアリング セッションを確立できます。EIGRP がルーティング更新を交換するインターフェイスは、ネイバー ステートメントで指定する必要があります。2 つの EIGRP ネイバーがルーティング更新を交換するインターフェイスは、同じネットワークにある IP アドレスで設定する必要があります。

（注） インターフェイスに対して **passive-interface** コマンドを設定すると、そのインターフェイスではすべての発着信ルーティング更新および hello メッセージが表示されなくなります。EIGRP ネイバーとの隣接関係は、パッシブとして設定されるインターフェイス経由で確立および維持できません。

EIGRP hello メッセージは、**neighbor** コマンドを使用して定義されたネイバーにユニキャスト メッセージとして送信されます。

例

次に、ネイバーを 192.168.1.1 および 192.168.2.2 として EIGRP ピアリング セッションを設定する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 192.168.0.0
```

```
hostname(config-router)# neighbor 192.168.1.1 interface outside
hostname(config-router)# neighbor 192.168.2.2 interface branch_office
```

関連コマンド

コマンド	説明
debug eigrp neighbors	EIGRP ネイバー メッセージに関するデバッグ情報を表示します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

nem

ハードウェア クライアントのネットワーク拡張モード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 **nem enable** コマンドを使用します。NEM をディセーブルにするには、**nem 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 NEM 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。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

nem {**enable | disable**}

no nem

構文の説明

disable	ネットワーク拡張モードをディセーブルにします。
enable	ネットワーク拡張モードをイネーブルにします。

デフォルト

ネットワーク拡張モード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	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

使用上のガイドライン

ネットワーク拡張モードを使用すると、ハードウェア クライアントは、VPN トンネルを介したリモート プライベート ネットワークへの単一のルーティング可能なネットワークを提供できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークからセキュリティ アプライアンスの背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、セキュリティ アプライアンスの背後にあるデバイスは、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。トンネルはハードウェア クライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、FirstGroup というグループ ポリシーの NEM を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

network

RIP ルーティング プロセスのネットワークのリストを指定するには、ルータ コンフィギュレーション モードで **network** コマンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

network *ip_addr*

no network *ip_addr*

構文の説明

ip_addr	直接接続されたネットワークの IP アドレス。指定されたネットワークに接続されているインターフェイスが、RIP ルーティング プロセスに参加します。

デフォルト

ネットワークは指定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

指定されたネットワーク番号は、サブネット情報に含めないでください。ルータで使用できる network コマンドの数に制限はありません。指定されたネットワーク上のインターフェイスのみを経由して、RIP ルーティング更新が送受信されます。また、インターフェイスのネットワークが指定されていない場合は、どの RIP ルーティング更新でもインターフェイスがアドバタイズされません。

例

次に、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されているすべてのインターフェイスで使用されるルーティング プロトコルとして RIP を定義する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# network 192.168.7.0
```

関連コマンド

コマンド	説明
router 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 router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

network（EIGRP）

EIGRP ルーティング プロセスのネットワークのリストを指定するには、ルータ コンフィギュレーション モードで **network** コマンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

network *ip_addr* [*mask*]

no network *ip_addr* [*mask*]

構文の説明

ip_addr	直接接続されたネットワークの IP アドレス。指定されたネットワークに接続されているインターフェイスが、EIGRP ルーティング プロセスに参加します。
mask	（任意）IP アドレスのネットワーク マスク。

デフォルト

ネットワークは指定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

network コマンドは、指定されたネットワークに IP アドレスが少なくとも 1 つ存在するすべてのインターフェイスで EIGRP を開始します。また、指定されたネットワークから接続済みのサブネットを EIGRP トポロジ テーブルに挿入します。

次に、セキュリティ アプライアンスは一致したインターフェイス経由でネイバーを確立します。セキュリティ アプライアンスに設定できる **network** コマンドの数に制限はありません。

例

次に、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されているすべてのインターフェイスで使用されるルーティング プロトコルとして EIGRP を定義する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0 255.0.0.0
hostname(config-router)# network 192.168.7.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp interfaces	EIGRP に設定されているインターフェイスに関する情報を表示します。
show eigrp topology	EIGRP トポロジ テーブルを表示します。

network-acl

access-list コマンドを使用して以前に設定したファイアウォールの ACL 名を指定するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **network-acl** コマンドを使用します。既存のネットワーク ACL を削除するには、このコマンドの **no** 形式を使用します。すべてのネットワーク ACL を削除するには、このコマンドを引数なしで使用します。

network-acl *name*

no network-acl [*name***]**

構文の説明

name	ネットワーク ACL の名前を指定します。最大 240 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

複数のファイアウォール ACL を DAP レコードに割り当てるには、このコマンドを複数回使用します。

セキュリティ アプライアンスは、指定された各 ACL を検証して、アクセス リスト エントリの許可ルールのみまたは拒否ルールのみが含まれていることを確認します。指定されたいずれかの ACL に許可ルールと拒否ルールが混在していた場合、セキュリティ アプライアンスはコマンドを拒否します。

次に、Finance Restrictions というネットワーク ACL を Finance という DAP レコードに適用する例を示します。

```
hostname(config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# network-acl Finance Restrictions
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
access-policy	ファイアウォール アクセス ポリシーを設定します。

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name***]**	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

network area

OSPF が動作するインターフェイスを定義し、そのインターフェイスのエリア ID を定義するには、ルータ コンフィギュレーション モードで **network area** コマンドを使用します。アドレス/ネットマスクのペアで定義されたインターフェイスの OSPF ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

network *addr mask* **area** *area_id*

no network *addr mask* **area** *area_id*

構文の説明

addr	[IP Address]。
area *area_id*	OSPF アドレス範囲に関連付けられるエリアを指定します。*area_id* は、IP アドレス形式または 10 進表記で指定できます。10 進表記で指定する場合、有効な値の範囲は、0 ～ 4294967295 です。
mask	ネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

インターフェイスで OSPF を動作させるには、インターフェイスのアドレスを **network area** コマンドの対象にする必要があります。**network area** コマンドがインターフェイスの IP アドレスを対象にしていない場合、そのインターフェイスを経由する OSPF はイネーブルになりません。

セキュリティ アプライアンスで使用できる **network area** コマンドの数に制限はありません。

例

次に、192.168.1.1 インターフェイスで OSPF をイネーブルにし、エリア 2 に割り当てる例を示します。

```
hostname(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

network-object

ネットワーク オブジェクトをネットワーク オブジェクト グループに追加するには、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用します。ネットワーク オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

network-object host *host_addr* | *host_name*

no network-object host *host_addr* | *host_name*

network-object *net_addr netmask*

no network-object *net_addr netmask*

構文の説明

host_addr	ホスト IP アドレス（ホスト名が **name** コマンドを使用してすでに定義されていない場合）。
host_name	ホスト名（ホスト名が **name** コマンドを使用して定義されている場合）。
net_addr	ネットワーク アドレス。サブネット オブジェクトを定義するために *netmask* とともに使用します。
netmask	ネットマスク。サブネット オブジェクトを定義するために *net_addr* とともに使用します。

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	透過	シングル	コンテキスト	システム
ネットワーク コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

network-object コマンドは、ネットワーク コンフィギュレーション モードでホストまたはサブネット オブジェクトを定義するために、**object-group** コマンドとともに使用します。

例

次に、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用して、新規にネットワーク オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group network sjj_eng_ftp_servers
hostname(config-network)# network-object host sjj.eng.ftp
hostname(config-network)# network-object host 172.16.56.195
hostname(config-network)# network-object 192.168.1.0 255.255.255.224
```

```
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# quit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

nt-auth-domain-controller

このサーバの NT プライマリ ドメイン コントローラ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 **nt-auth-domain-controller** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

nt-auth-domain-controller *string*

no nt-auth-domain-controller

構文の説明

string	このサーバのプライマリ ドメイン コントローラの名前を最大 16 文字で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、NT 認証 AAA サーバに対してのみ有効です。ホスト コンフィギュレーション モードを開始するには、**aaa-server host** コマンドを先に使用する必要があります。*string* 変数の名前は、そのサーバ自体の NT エントリに一致する必要があります。

例

次に、このサーバの NT プライマリ ドメイン コントローラの名前を「primary1」に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol nt
hostname(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。

clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

ntp authenticate

NTP サーバによる認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ntp authenticate** コマンドを使用します。NTP 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ntp authenticate

no ntp authenticate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

認証をイネーブルにした場合、NTP サーバがパケットで正しい信頼できるキーを使用しているのであれば（**ntp trusted-key** コマンドを参照）、セキュリティ アプライアンスはその NTP サーバとのみ通信します。また、セキュリティ アプライアンスは認証キーを使用して NTP サーバと同期します（**ntp authentication-key** コマンドを参照）。

例

次に、NTP パケットで認証キー 42 を提供するシステムにのみ同期するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp authentication-key 42 md5 aNiceKey
hostname(config)# ntp trusted-key 42
```

関連コマンド

コマンド	説明
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。

コマンド	説明
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp authentication-key

NTP サーバで認証するキーを設定するには、グローバル コンフィギュレーション モードで **ntp authentication-key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

ntp authentication-key *key_id* **md5** *key*

no ntp authentication-key *key_id* [**md5** *key*]

構文の説明

key_id	キー ID 1 ～ 4294967295 を識別します。この ID は、**ntp trusted-key** コマンドを使用して信頼できるキーとして指定する必要があります。
md5	認証アルゴリズムを MD5 として指定します。サポートされている唯一のアルゴリズムが MD5 です。
key	キー値を最大 32 文字のストリングとして設定します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 および 2 を指定して、信頼できる各キーの認証キーを設定します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp server

NTP サーバを指定して、セキュリティ アプライアンス上の時間を設定するには、グローバル コンフィギュレーション モードで **ntp server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。複数のサーバを識別できます。セキュリティ アプライアンス では、最も正確なサーバを使用します。マルチ コンテキスト モードでは、システム コンフィギュレーションにのみ NTP サーバを設定します。

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

no ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

構文の説明

ip_address	NTP サーバの IP アドレスを設定します。
key *key_id*	**ntp authenticate** コマンドを使用して認証をイネーブルにした場合は、このサーバの信頼できるキー ID を設定します。**ntp trusted-key** コマンドも参照してください。
source *interface_name*	ルーティング テーブルにデフォルトのインターフェイスを使用しない場合に、NTP パケットの発信インターフェイスを識別します。マルチ コンテキスト モードではシステムにインターフェイスが含まれないため、管理コンテキストに定義されているインターフェイス名を指定します。
prefer	精度に差がないサーバが複数ある場合は、この NTP サーバを優先サーバとして設定します。NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。サーバの精度に差がない場合は、**prefer** キーワードにどのサーバを使用するかを指定します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、セキュリティ アプライアンス では、精度の高いそのサーバを使用します。たとえば、セキュリティ アプライアンスは優先サーバであるストラタム 3 サーバよりもストラタム 2 のサーバを優先的に使用します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、送信元インターフェイスを任意とするように変更されました。

例

次に、2 つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
hostname(config)# ntp server 10.1.1.1 key 1 prefer
hostname(config)# ntp server 10.2.1.1 key 2
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp trusted-key

NTP サーバによる認証を必要とする信頼できるキーに認証キー ID 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 **ntp trusted-key** コマンドを使用します。信頼できるキーを削除するには、このコマンドの **no** 形式を使用します。複数のサーバで使用できるように複数の信頼できるキーを入力できます。

ntp trusted-key *key_id*

no ntp trusted-key *key_id*

構文の説明

key_id	キー ID 1 ～ 4294967295 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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。サーバと同期するには、**ntp authentication-key** コマンドを使用して、キー ID の認証キーを設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 および 2 を指定して、信頼できる各キーの認証キーを設定します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。

コマンド	説明
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

num-packets

SLA 動作中に送信される要求パケットの数を指定するには、SLA モニタ プロトコル コンフィギュレーション モードで **num-packets** 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。

num-packets *number*

no num-packets *number*

構文の説明

number	SLA 動作中に送信されるパケットの数。有効な値は、1 ～ 100 です。

デフォルト

エコー タイプの場合に送信されるデフォルトのパケット数は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

パケット損失のために到達可能性情報が不正確になるのを防ぐには、送信されるデフォルトのパケット数を増やします。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。この例では、エコー要求パケットのペイロード サイズを 48 バイト、SLA 動作中に送信されるエコー要求の数を 5 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

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

object-group

コンフィギュレーションの最適化に使用できるオブジェクト グループを定義するには、グローバル コンフィギュレーション モードで **object-group** コマンドを使用します。コンフィギュレーションからオブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

no object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

object-group service *obj_grp_id* [**tcp** | **udp** | **tcp-udp**]

no object-group service *obj_grp_id* [**tcp** | **udp** | **tcp-udp**]

構文の説明

icmp-type	echo や echo-reply など ICMP タイプのグループを定義します。メインの **object-group icmp-type** コマンドを入力した後、**icmp-object** コマンドおよび **group-object** コマンドで ICMP オブジェクトを ICMP タイプ グループに追加します。
network	ホストまたはサブネットの IP アドレスのグループを定義します。メインの **object-group network** コマンドを入力した後、**network-object** コマンドおよび **group-object** コマンドでネットワーク オブジェクトをネットワーク グループに追加します。
obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。文字、数字、および「_」、「-」、「.」の組み合わせが使用可能です。
protocol	TCP や UDP などプロトコルのグループを定義します。メインの **object-group protocol** コマンドを入力した後、**protocol-object** コマンドと **group-object** コマンドを使用して、プロトコル オブジェクトをプロトコル グループに追加します。
service	拡張サービス オブジェクト グループの定義には、TCP サービス、UDP サービス、ICMP-type サービス、および（コマンドラインに **tcp**、**udp**、または **tcp-udp** が指定されていない場合には）プロトコルを混在させることができます。メインの **object-group service** コマンドを入力した後、**service-object** コマンドと **group-object** コマンドを使用して、サービス オブジェクトをサービス グループに追加します。 **tcp**、**udp**、または **tcp-udp** が任意でコマンドラインに指定されている場合、**service** には「eq smtp」や「range 2000 2010」など TCP/UDP ポート仕様の標準のサービス オブジェクト グループを定義します。この場合、メインの **object-group service** コマンドを入力した後、**port-object** コマンドと **group-object** コマンドを使用して、ポート オブジェクトをサービス グループに追加します。
tcp	サービス グループが TCP に使用されることを指定します。
tcp-udp	サービス グループが TCP および UDP に使用できることを指定します。
udp	サービス グループが UDP に使用されることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　ホスト、プロトコル、サービスなどのオブジェクトを 1 つのグループにまとめてから、そのグループ名を使用して、グループ内の各項目に適用する単一のコマンドを発行できます。

object-group コマンドでグループを定義してから任意のセキュリティ アプライアンス コマンドを使用すると、そのコマンドはグループ内の各項目に適用されます。この機能を使用すると、コンフィギュレーションのサイズを大幅に削減できます。

オブジェクト グループを定義したときは、適用可能なすべてのセキュリティ アプライアンス コマンドで次のようにグループ名の前に **object-group** キーワードを使用する必要があります。

```
hostname# show running-config object-group group_name
```

group_name はグループの名前です。

次に、オブジェクト グループを定義してから使用する例を示します。

```
hostname(config)# access-list access_list_name permit tcp any object-group group_name
```

また、**access-list** コマンド引数をグループ化できます。

個々の引数	オブジェクト グループの置き換え
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp_type	**object-group** *icmp_type*

コマンドを階層的にグループ化できます。つまり、オブジェクト グループを別のオブジェクト グループのメンバーにすることができます。

オブジェクト グループを使用するには、次の手順を実行する必要があります。

- すべてのコマンドで次のようにオブジェクト グループ名の前に **object-group** キーワードを使用します。

  ```
  hostname(config)# access-list acl permit tcp object-group remotes object-group locals
  object-group eng_svc
  ```

  remotes および *locals* は、サンプルのオブジェクト グループ名です。
- オブジェクト グループは空にできません。

- コマンドで現在使用されているオブジェクト グループは削除することも、空にすることもできません。

メインの **object-group** コマンドを入力した後、コマンド モードは対応するモードに変わります。オブジェクト グループは、変更後のモードに定義されます。アクティブ モードは、コマンド プロンプト形式で示されます。たとえば、コンフィギュレーション ターミナル モードのプロンプトは、次のように表示されます。

```
hostname(config)#
```

ここで *hostname* は、セキュリティ アプライアンスの名前です。

ただし、**object-group** コマンドを入力すると、プロンプトは次のように表示されます。

```
hostname(config-type)#
```

ここで *hostname* はセキュリティ アプライアンスの名前で、*type はオブジェクト グループのタイプです。*

object-group モードを終了し、メインの **object-group** コマンドを実行するには、**exit** か **quit**、あるいは **access-list** などその他の有効なコンフィギュレーション モード コマンドを使用します。

show running-config object-group コマンドは、定義済みのすべてのオブジェクト グループを、**show running-config object-group** *grp_id* コマンドが入力されたときには *grp_id* 別に表示し、**show running-config object-group** *grp_type* コマンドが入力されたときにはグループ タイプ別に表示します。**show running-config object-group** コマンドを引数なしで入力すると、定義済みのすべてのオブジェクト グループが表示されます。

以前に定義した **object-group** コマンドのグループを削除するには、**clear configure object-group** コマンドを使用します。引数なしで **clear configure object-group** コマンドを使用すると、コマンドに現在使用されていない定義済みのすべてのオブジェクト グループを削除できます。*grp_type* 引数は、そのグループ タイプのみを対象に、コマンドに使用されていない定義済みのすべてのオブジェクト グループを削除します。

show running-config や **clear configure** など他のすべてのセキュリティ アプライアンス コマンドをオブジェクト グループ モードで使用できます。

オブジェクト グループ モード内のコマンドは、**show running-config object-group**、**write**、または **config** コマンドによって表示または保存されるときにインデントされます。

オブジェクト グループ モード内のコマンドは、コマンド特権レベルがメインのコマンドと同じレベルになります。

access-list コマンドで複数のオブジェクト グループを使用するときには、コマンドに使用されるすべてのオブジェクト グループの要素がリンクされます。最初のグループの要素が 2 つめのグループの要素とリンクされ、続いて最初と 2 つめのグループの要素がともに 3 つのグループの要素にリンクされ、以後同じようにリンクされます。

説明テキストの開始位置は、**description** キーワードに続くスペース（ブランクまたはタブ）の直後の文字となります。

例

次に、**オブジェクト グループ ICMP-type** モードを使用して、新規に ICMP-type オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group icmp-type icmp-allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

次に、**object-group network** コマンドを使用して、新規にネットワーク オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group network sjc_eng_ftp_servers
hostname(config-network)# network-object host sjc.eng.ftp.servcers
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object 192.1.1.0 255.255.255.224
hostname(config-network)# exit
```

次に、**object-group network** コマンドを使用して、新規にネットワーク オブジェクト グループを作成し、それを既存のオブジェクト グループにマッピングする例を示します。

```
hostname(config)# object-group network sjc_ftp_servers
hostname(config-network)# network-object host sjc.ftp.servers
hostname(config-network)# network-object host 172.23.56.195
hostname(config-network)# network-object 193.1.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# exit
```

次に、**オブジェクト グループ プロトコル** モードを使用して、新規にプロトコル オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object ipsec
hostname(config-protocol)# exit

hostname(config)# object-group protocol proto_grp_2
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
```

次に、**オブジェクト グループ サービス** モードを使用して、新規にポート（サービス）オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# group-object eng_www_service
hostname(config-service)# port-object eq ftp
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# exit
```

次に、オブジェクト グループに対してテキスト説明を追加および削除する例を示します。

```
hostname(config)# object-group protocol protos1
hostname(config-protocol)# description This group of protocols is for our internal network

hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
description: This group of protocols is for our internal network

hostname(config-protocol)# no description
hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
```

次に、**グループ オブジェクト** モードを使用して、以前に定義したオブジェクトで構成されているオブジェクト グループを新規に作成する例を示します。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit

hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
```

```
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit

hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)#access-list all permit tcp object-group all_hosts any eq www
```

group-object コマンドを指定しないときは、*host_grp_1* および *host_grp_2* にすでに定義されているすべての IP アドレスが含まれるように、*all_hosts* グループを定義する必要があります。**group-object** コマンドを指定すると、重複するホストの定義が削除されます。

次に、オブジェクト グループを使用して、アクセス リスト コンフィギュレーションを簡素化する例を示します。

```
hostname(config)# object-group network remote
hostname(config-network)# network-object host kqk.suu.dri.ixx
hostname(config-network)# network-object host kqk.suu.pyl.gnl

hostname(config)# object-group network locals
hostname(config-network)# network-object host 209.165.200.225
hostname(config-network)# network-object host 209.165.200.230
hostname(config-network)# network-object host 209.165.200.235
hostname(config-network)# network-object host 209.165.200.240

hostname(config)# object-group service eng_svc tcp
hostname(config-service)# port-object eq www
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object range 25000 25100
```

グループ化を使用しないとアクセス リストの設定には 24 行必要ですが、このグループ化により、1 行で設定できます。グループ化を使用した場合、アクセス リスト コンフィギュレーションは次のようになります。

```
hostname(config)# access-list acl permit tcp object-group remote object-group locals
object-group eng_svc
```

次に、**service-object** サブコマンドを使用する例を示します。このサブコマンドは、TCP サービスおよび UDP サービスをグループ化する場合に便利です。

```
hostname(config)# object-group network remote
hostname(config-network)# network-object host kqk.suu.dri.ixx
hostname(config-network)# network-object host kqk.suu.pyl.gnl

hostname(config)# object-group network locals
hostname(config-network)# network-object host host 209.165.200.225
hostname(config-network)# network-object host host 209.165.200.230
hostname(config-network)# network-object host host 209.165.200.235
hostname(config-network)# network-object host host 209.165.200.240

hostname(config)# object-group service usr_svc
hostname(config-service)# service-object tcp eq www
hostname(config-service)# service-object tcp eq https
hostname(config-service)# service-object tcp eq pop3
hostname(config-service)# service-object udp eq ntp
hostname(config-service)# service-object udp eq domain

hostname(config)# access-list acl permit object-group usr_svc object-group locals
object-group remote
```

（注）　**show running-config object-group** コマンドおよび **write** コマンドを使用すると、オブジェクト グループ名で設定したとおりにアクセス リストを表示できます。**show access-list** コマンドは、オブジェクト グループ化なしで個々のエントリに展開されるアクセス リスト エントリを表示します。

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

ocsp disable-nonce

ナンス拡張をディセーブルにするには、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 **ocsp disable-nonce** コマンドを使用します。デフォルトでは、OCSP 要求にナンス拡張が含まれています。ナンス拡張は、暗号化によって要求を応答にバインドし、リプレイ アタックを回避します。ただし、OCSP サーバによっては、この一致するナンス拡張が含まれていない事前生成の応答が使用される場合があります。このようなサーバで OCSP を使用するには、ナンス拡張をディセーブルにする必要があります。ナンス拡張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。

ocsp disable-nonce

no ocsp disable-nonce

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトでは、OCSP 要求にナンス拡張が含まれています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するとき、OCSP 要求には OCSP ナンス拡張が含まれず、セキュリティ アプライアンスは OCSP ナンス拡張をチェックしません。

例

次に、newtrust というトラストポイントのナンス拡張をディセーブルにする例を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp disable-nonce
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書きルールを設定します。

コマンド	説明
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバを指定します。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

ocsp url

クライアント証明書の AIA 拡張で指定されたサーバではなく、セキュリティ アプライアンスの OCSP サーバを、トラストポイントに関連付けられたすべての証明書のチェックに使用するように設定するには、暗号 CA トラストポイント コンフィギュレーション モードで **ocsp url** コマンドを使用します。このサーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ocsp url *URL*

no ocsp url

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、HTTP URL のみをサポートし、トラストポイントごとに URL を 1 つだけ指定できます。

セキュリティ アプライアンスでは 3 つの方法で OCSP サーバの URL を定義でき、その定義方法に従って次の順序で OCSP サーバの使用を試みます。

- **match certificate** コマンドで設定された OCSP サーバ。
- **ocsp url** コマンドで設定された OCSP サーバ。
- クライアント証明書の AIA フィールドに指定された OCSP サーバ。

match certificate コマンドまたは **ocsp url** コマンドで OCSP URL を設定しないと、セキュリティ アプライアンスはクライアント証明書の AIA 拡張に指定された OCSP サーバを使用します。証明書に AIA 拡張がない場合、失効ステータスのチェックは失敗します。

例

次に、URL http://10.1.124.22 で OCSP サーバを設定する例を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp url http://10.1.124.22
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書きルールを設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

onscreen-keyboard

ログイン/パスワード要件とともにオンスクリーン キーボードをログイン ペインまたはすべてのペインに挿入するには、webvpn モードで **onscreen-keyboard** コマンドを使用します。以前に設定したオンスクリーン キーボードを削除するには、このコマンドの **no** 形式を使用します。

onscreen-keyboard {logon | all}

no onscreen-keyboard [logon | all]

構文の説明

logon	ログイン ペインのオンスクリーン キーボードを挿入します。
all	ログイン/パスワードの要件とともに、ログイン ペインおよび他のすべてのペインのオンスクリーン キーボードを挿入します。

デフォルト

オンスクリーン キーボードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

オンスクリーン キーボードを使用すると、キーストロークなしでユーザ クレデンシャルを入力できます。

例

次に、ログイン ページのオンスクリーン キーボードをイネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# onscreen-keyboard logon
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn モードを開始し、クライアントレス SSLVPN 接続の属性を設定できるようにします。

ospf authentication

OSPF 認証の使用を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 **ospf authentication** コマンドを使用します。デフォルトの認証状態に戻すには、このコマンドの **no** 形式を使用します。

ospf authentication [**message-digest** | **null**]

no ospf authentication

構文の説明

message-digest	（任意）OSPF メッセージ ダイジェスト認証を使用することを指定します。
null	（任意）OSPF 認証を使用しないことを指定します。

デフォルト

デフォルトでは、OSPF 認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	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf authentication コマンドを使用する前に、**ospf authentication-key** コマンドを使用してインターフェイスのパスワードを設定します。**message-digest** キーワードを使用する場合は、**ospf message-digest-key** コマンドを使用して、インターフェイスのメッセージ ダイジェスト キーを設定します。

下位互換性を確保するため、エリアの認証タイプは引き続きサポートされます。インターフェイスの認証タイプを指定しないと、エリアの認証タイプが使用されます（エリアのデフォルトはヌル認証です）。

このコマンドをオプションなしで使用すると、簡易パスワード認証がイネーブルになります。

例

次に、選択したインターフェイスで OSPF の簡易パスワード認証をイネーブルにする例を示します。

```
hostname(config-if)# ospf authentication
hostname(config-if)#
```

関連コマンド

コマンド	説明
ospf authentication-key	ネイバー ルーティング デバイスで使用されるパスワードを指定します。
ospf message-digest-key	MD5 認証をイネーブルにし、MD5 キーを指定します。

ospf authentication-key

ネイバー ルーティング デバイスで使用されるパスワードを指定するには、インターフェイス コンフィギュレーション モードで **ospf authentication-key** コマンドを使用します。パスワードを削除するには、このコマンドの **no** 形式を使用します。

ospf authentication-key *password*

no ospf authentication-key

構文の説明

password	ネイバー ルーティング デバイスで使用される OSPF 認証パスワードを割り当てます。パスワードは、9 文字未満にする必要があります。2 文字間にブランクを含めることができます。パスワードの先頭または末尾のブランクは無視されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドが作成するパスワードは、ルーティング プロトコル パケットの送信時に、OSPF ヘッダーに直接挿入されるキーとして使用されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

例

次に、OSPF 認証のパスワードを指定する例を示します。

```
hostname(config-if)# ospf authentication-key ThisMyPW
```

関連コマンド

コマンド	説明
area authentication	指定したエリアの OSPF 認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf cost

インターフェイス経由でパケットを送信するコストを指定するには、インターフェイス コンフィギュレーション モードで **ospf cost** コマンドを使用します。インターフェイス コストをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

ospf cost *interface_cost*

no ospf cost

構文の説明

interface_cost	インターフェイス経由でパケットを送信するコスト（リンクステート メトリック）。これは、符号なし整数値 0 ～ 65535 です。0 はインターフェイスに直接接続されているネットワークを表し、インターフェイス帯域幅が大きくなるほど、そのインターフェイス経由のパケット送信に伴うコストは低くなります。つまり、コストの値が大きければインターフェイス帯域幅が小さく、コストの値が小さければインターフェイス帯域幅が大きいということになります。 セキュリティ アプライアンスでの OSPF インターフェイスのデフォルトのコストは 10 です。このデフォルトは、Cisco IOS ソフトウェアとは異なります。Cisco IOS ソフトウェアの場合、デフォルトのコストはファスト イーサネットおよびギガビット イーサネットでは 1、10BaseT では 10 です。ネットワークで ECMP を使用している場合には、このことを考慮に入れることが重要です。

デフォルト

デフォルトの *interface_cost* は、10 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf cost コマンドを使用すると、インターフェイスでパケットを送信するコストを明示的に指定できます。*interface_cost* パラメータは、符号なし整数値 0 ～ 65535 です。

no ospf cost コマンドを使用すると、パス コストをデフォルト値にリセットできます。

例

次に、選択したインターフェイスでパケットを送信するコストを指定する例を示します。

```
hostname(config-if)# ospf cost 4
```

関連コマンド

コマンド	説明
show running-config interface	指定したインターフェイスの設定を表示します。

ospf database-filter

同期およびフラッディング時に OSPF インターフェイスへの発信 LSA をすべてフィルタリングするには、インターフェイス コンフィギュレーション モードで **ospf database-filter** コマンドを使用します。LSA を復元するには、このコマンドの **no** 形式を使用します。

ospf database-filter all out

no ospf database-filter all out

構文の説明

all out	OSPF インターフェイスへの発信 LSA をすべてフィルタリングします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf database-filter コマンドは、OSPF インターフェイスへの発信 LSA をフィルタリングします。**no ospf database-filter all out** コマンドは、インターフェイスへの LSA の転送を復元します。

例

次に、**ospf database-filter** コマンドを使用して、発信 LSA をフィルタリングする例を示します。

```
hostname(config-if)# ospf database-filter all out
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf dead-interval

ネイバーがルータのダウンを宣言するまでの間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf dead-interval** 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。

ospf dead-interval *seconds*

no ospf dead-interval

構文の説明

seconds	hello パケットが確認されない時間の長さ。*seconds* のデフォルトは、**ospf hello-interval** コマンドによって設定される間隔（1 ～ 65535）の 4 倍です。

デフォルト

seconds のデフォルト値は、**ospf hello-interval** コマンドによって設定される間隔の 4 倍です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf dead-interval コマンドを使用すると、ネイバーがルータのダウンを宣言するまでのデッド間隔（no hello パケットが確認されない時間の長さ）を設定できます。*seconds* 引数にはデッド間隔を指定し、その値はネットワーク上のすべてのノードで同じである必要があります。*seconds* のデフォルトは、**ospf hello-interval** コマンドによって設定される間隔（1 ～ 65535）の 4 倍です。

no ospf dead-interval コマンドは、デフォルトの間隔値を復元します。

例

次に、OSPF デッド間隔を 1 分に設定する例を示します。

```
hostname(config-if)# ospf dead-interval 60
```

関連コマンド

コマンド	説明
ospf hello-interval	インターフェイス上での hello パケットの送信間隔を指定します。
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf hello-interval

インターフェイス上での hello パケットの送信間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf hello-interval** コマンドを使用します。hello 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。

ospf hello-interval *seconds*

no ospf hello-interval

構文の説明

seconds	インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。

デフォルト

hello-interval *seconds* のデフォルト値は、10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

この値は、hello パケットでアドバタイズされます。hello 間隔を小さくするほど、トポロジの変更が速く検出されますが、ルーティング トラフィックの増加につながります。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。

例

次に、OSPF hello 間隔を 5 秒に設定する例を示します。

```
hostname(config-if)# ospf hello-interval 5
```

関連コマンド

コマンド	説明
ospf dead-interval	ネイバーがルータのダウンを宣言するまでの間隔を指定します。
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf message-digest-key

OSPF MD5 認証を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 **ospf message-digest-key** コマンドを使用します。MD5 キーを削除するには、このコマンドの **no** 形式を使用します。

ospf message-digest-key *key-id* **md5** *key*

no ospf message-digest-key

構文の説明

key-id	MD5 認証をイネーブルにし、認証キー ID 番号を数値で指定します。有効な値は、1 ～ 255 です。
md5 *key*	最大 16 バイトの英数字のパスワード。キーの文字間にスペースを含めることができます。キーの先頭または末尾のスペースは無視されます。MD5 認証は、通信の整合性を検証し、発信元を認証し、適時性をチェックします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf message-digest-key コマンドを使用すると、MD5 認証をイネーブルにできます。このコマンドの **no** 形式を使用すると、古い MD5 キーを削除できます。*key_id* は、認証キーを識別する 1 ～ 255 の数値です。*key* は、最大 16 バイトの英数字のパスワードです。MD5 は通信の整合性を確認し、発信元を認証して、適時性をチェックします。

例

次に、OSPF 認証の MD5 キーを指定する例を示します。

```
hostname(config-if)# ospf message-digest-key 3 md5 ThisIsMyMd5Key
```

関連コマンド

コマンド	説明
area authentication	OSPF エリア認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf mtu-ignore

受信データベース パケットで OSPF 最大伝送単位（MTU）ミスマッチ検出をディセーブルにするには、インターフェイス コンフィギュレーション モードで **ospf mtu-ignore** コマンドを使用します。MTU ミスマッチ検出を復元するには、このコマンドの **no** 形式を使用します。

ospf mtu-ignore

no ospf mtu-ignore

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、**ospf mtu-ignore** はイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーが Database Descriptor（DBD; データベース記述子）パケットを交換するときに実行されます。DBD パケットの受信 MTU が、着信インターフェイスに設定されている IP MTU よりも高くなっている場合、OSPF 隣接は確立されません。**ospf mtu-ignore** コマンドは、受信 DBD パケットで OSPF MTU ミスマッチ検出をディセーブルにします。デフォルトではイネーブルです。

例

次に、**ospf mtu-ignore** コマンドをディセーブルにする例を示します。

```
hostname(config-if)# ospf mtu-ignore
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf network point-to-point non-broadcast

OSPF インターフェイスをポイントツーポイントの非ブロードキャスト ネットワークとして設定するには、インターフェイス コンフィギュレーション モードで **ospf network point-to-point non-broadcast** コマンドを使用します。コンフィギュレーションからこのコマンドを削除するには、このコマンドの **no** 形式を使用します。**ospf network point-to-point non-broadcast** コマンドを使用すると、VPN トンネルで OSPF ルートを送信できます。

ospf network point-to-point non-broadcast

no ospf network point-to-point non-broadcast

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスをポイントツーポイントとして指定したときは、OSPF ネイバーを手動で設定する必要があります。ダイナミック探索は機能しません。OSPF ネイバーを手動で設定するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。

インターフェイスをポイントツーポイントとして設定したときには、次の制約事項が適用されます。

- インターフェイスにはネイバーを 1 つだけ定義できます。
- クリプト ポイントを指すスタティック ルートを定義する必要があります。
- ネイバーを明示的に設定しない限り、インターフェイスは隣接を形成できません。
- トンネル経由の OSPF がインターフェイスで実行中である場合は、その同じインターフェイスでは上流のルータがある通常の OSPF を実行できません。
- OSPF 更新が VPN トンネルを通過できるように、OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。OSPF ネイバーを指定した後でクリプト マップをインターフェイスにバインドした場合は、OSPF 隣接を VPN トンネル経由で確立できるように、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。

例

次に、選択したインターフェイスをポイントツーポイントの非ブロードキャスト インターフェイスとして設定する例を示します。

```
hostname(config-if)# ospf network point-to-point non-broadcast
hostname(config-if)#
```

関連コマンド

コマンド	説明
neighbor	手動で設定した OSPF ネイバーを指定します。
show interface	インターフェイスのステータス情報を表示します。

ospf priority

OSPF ルータのプライオリティを変更するには、インターフェイス コンフィギュレーション モードで **ospf 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。

ospf priority *number*

no ospf priority [*number*]

構文の説明

number	ルータのプライオリティを指定します。有効な値は、0 ～ 255 です。

デフォルト

number のデフォルト値は、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	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ネットワークにアタッチされている 2 つのルータがともに指定ルータになろうとした場合、ルータのプライオリティの高い方が優先されます。プライオリティが同じ場合、より高位のルータ ID を持つルータが優先されます。ルータのプライオリティがゼロに設定されているルータには、指定ルータまたはバックアップ指定ルータになる資格がありません。ルータのプライオリティは、マルチアクセス ネットワークへのインターフェイス専用に設定されます（つまり、ポイントツーポイント ネットワークへのインターフェイスには設定されません）。

例

次に、選択したインターフェイスで OSPF プライオリティを変更する例を示します。

```
hostname(config-if)# ospf priority 4
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf retransmit-interval

インターフェイスに属する隣接の LSA 再送信間の時間を指定するには、インターフェイス コンフィギュレーション モードで **ospf retransmit-interval** 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。

ospf retransmit-interval *seconds*

no ospf retransmit-interval [*seconds*]

構文の説明

seconds	インターフェイスに属する隣接ルータの LSA 再送信間の時間を指定します。有効な値は、1 ～ 65535 秒です。

デフォルト

retransmit-interval *seconds* のデフォルト値は、5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答メッセージを受信しないと、ルータは LSA を再送信します。

このパラメータの設定値は控えめにする必要があります。そうしないと、不要な再送信が発生します。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

例

次に、LSA の再送信間隔を変更する例を示します。

```
hostname(config-if)# ospf retransmit-interval 15
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf transmit-delay

インターフェイス上でリンクステート更新パケットを送信するために必要とされる時間を設定するには、インターフェイス コンフィギュレーション モードで **ospf transmit-delay** 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。

ospf transmit-delay *seconds*

no ospf transmit-delay [*seconds*]

構文の説明

seconds	インターフェイス上でリンクステート更新パケットを送信するために必要とされる時間を設定します。デフォルト値は 1 秒で、有効な値の範囲は 1 ～ 65535 秒です。

デフォルト

seconds のデフォルト値は、1 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

更新パケット内の LSA には、送信前に、*seconds* 引数で指定した値によって増加された経過時間が格納されます。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。

リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。この設定は、非常に低速のリンクでより重要な意味を持ちます。

例

次に、選択したインターフェイスの送信遅延を 3 秒に設定する例を示します。

```
hostname(config-if)# ospf restransmit-delay 3
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

otp expiration

ローカル Certificate Authority（CA; 認証局）登録ページ用に発行されたワンタイム パスワード（OTP）の有効期間を時間単位で指定するには、CA サーバ コンフィギュレーション モードで **otp expiration** コマンドを使用します。期間をデフォルトの時間数にリセットするには、このコマンドの **no** 形式を使用します。

otp expiration *timeout*

no otp expiration

構文の説明

timeout	登録ページ用の OTP が期限切れになる前に、ユーザがローカル CA から証明書を登録する必要がある期間を時間単位で指定します。有効な値の範囲は、1 ～ 720 時間（30 日）です。

デフォルト

デフォルトでは、証明書登録用の OTP の有効期限は 72 時間（3 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	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

OTP の有効期限には、ユーザが CA サーバの登録ページにログインする必要がある時間数を指定します。ユーザがログインし、証明書を登録すると、**enrollment retrieval** コマンドで指定された期間が開始されます。

（注） 登録インターフェイス ページで証明書を登録するためのユーザ OTP は、そのユーザの発行済みの証明書とキー ペアが含まれている PKCS12 ファイルをアンロックするためのパスワードとしても使用されます。

例

次に、登録ページ用の OTP が 24 時間適用されることを指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# otp expiration 24
hostname(config-ca-server)#
```

次に、OTP 期間をデフォルトの 72 時間にリセットする例を示します。

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

```
hostname(config-ca-server))# no otp expiration
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
enrollment-retrieval	登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。
show crypto ca server	認証局コンフィギュレーションを表示します。

outstanding

認証されていない電子メール プロキシ セッションの数を制限するには、適用可能な電子メール プロキシ コンフィギュレーション モードで **outstanding** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。

outstanding {*number*}

no outstanding

構文の説明

number	認証されていないセッションを許可する数。範囲は 1 ～ 1000 です。

デフォルト

デフォルト値は 20 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

認証されていないセッションを許可する数に制限がないコンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。これは、電子メール ポートに対する DoS 攻撃も制限します。

電子メール プロキシ接続には、3 つの状態があります。

1. 新規に電子メール接続が確立されると、「認証されていない」状態になります。
2. この接続でユーザ名が提示されると、「認証中」状態になります。
3. セキュリティ アプライアンスが接続を認証すると、「認証済み」状態になります。

認証されていない状態の接続の数が設定済みの制限値を超えた場合、セキュリティ アプライアンスは認証されていない接続のうち最も古いものを終了して、過負荷を回避します。認証済みの接続は終了しません。

例

次に、POP3S 電子メール プロキシの認証されていないセッションの制限を 12 に設定する例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# outstanding 12
```

override-account-disable

AAA サーバからの account-disabled インジケータを上書きするには、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 **override-account-disable** コマンドを使用します。上書き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。

override-account-disable

no override-account-disable

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	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、NT LDAP がある RADIUS や Kerberos など、「account-disabled」インジケータを返すサーバに有効です。

IPSec RA および WebVPN トンネル グループにこの属性を設定できます。

例

次に、「testgroup」という WebVPN トンネル グループについて AAA サーバからの「account-disabled」インジケータの上書きを許可する例を示します。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

次に、「QAgroup」という IPSec リモート アクセス トンネル グループについて AAA サーバからの「account-disabled」インジケータの上書きを許可する例を示します。

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	特定のトンネル グループのトンネル グループ データベースまたはコンフィギュレーションをクリアします。
tunnel-group general-attributes	トンネル グループ一般属性値を設定します。

override-svc-download

AnyConnect クライアントまたは SSL VPN クライアントをダウンロードするためのグループ ポリシーまたはユーザ名属性コンフィギュレーションを上書きするように接続プロファイルを設定するには、トンネル グループ webvpn 属性コンフィギュレーション モードで **override-svc-download** コマンドを使用します。コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

override-svc-download enable

no override-svc-download enable

デフォルト

デフォルトではディセーブルになっています。セキュリティ アプライアンスは、クライアントをダウンロードするためのグループ ポリシーまたはユーザ名属性コンフィギュレーションを上書きしません。

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	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、**vpn-tunnel-protocol** コマンドによってグループ ポリシーまたはユーザ名属性でクライアントレスか SSL VPN またはその両方がイネーブルになっているかどうかに基づいて、リモート ユーザに対してクライアントレス接続、AnyConnect 接続、または SSL VPN クライアント接続を許可します。**svc ask** コマンドはさらに、クライアントをダウンロードするか、または WebVPN ホームページに戻るようにユーザに要求して、クライアントのユーザ エクスペリエンスを変更します。

ただし、特定のトンネル グループのもとでログインしているクライアントレス ユーザが、ダウンロードの要求が期限切れになってクライアントレス SSL VPN ホームページが表示されるまで待たなくてもよいようにすることを推奨します。**override-svc-download** コマンドを使用すると、接続プロファイル レベルでこのようなユーザに対する遅延を防止できます。このコマンドにより、接続プロファイル経由でログインするユーザには、**vpn-tunnel-protocol** コマンドまたは **svc ask** コマンドの設定に関係なく、ただちにクライアントレス SSL VPN ホームページが表示されるようになります。

例

次の例では、ユーザは接続プロファイル *engineering* のトンネル グループ webvpn 属性コンフィギュレーション モードを開始し、この接続プロファイルでクライアントのダウンロード要求に関するグループ ポリシーおよびユーザ名属性の設定を上書きしています。

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# override-svc-download
```

関連コマンド

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