CHAPTER 11

default（crl configure）コマンド～ dynamic-access-policy-record コマンド

default（crl 設定）

すべての CRL パラメータをシステム デフォルト値に戻すには、crl 設定コンフィギュレーション モードで **default** コマンドを使用します。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバで必要な場合のみ使用されます。

default

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
crl 設定コンフィギュレーション	•		•		

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。

例

次に、ca-crl コンフィギュレーション モードを開始して、CRL コマンド値をデフォルトに戻す例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# default
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードを開始します。
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。
protocol ldap	CRL の取得方法として LDAP を指定します。

default（インターフェイス）

インターフェイス コマンドをシステム デフォルト値に戻すには、インターフェイス コンフィギュレーション モードで **default** コマンドを使用します。

default *command*

構文の説明

command	デフォルトに設定するコマンドを指定します。次に例を示します。 `default activation key`

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

このコマンドは実行時コマンドです。入力しても、アクティブなコンフィギュレーションの一部になりません。

例

次に、インターフェイス コンフィギュレーション モードを開始して、セキュリティ レベルをデフォルトに戻す例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# default security-level
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

default（時間範囲）

absolute コマンドおよび **periodic** コマンドの設定をデフォルトに戻すには、時間範囲コンフィギュレーション モードで **default** コマンドを使用します。

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

構文の説明

absolute	時間範囲が有効になる絶対時間を定義します。
days-of-the-week	最初の days-of-the-week 引数は、関連付けられている有効時間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。 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。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 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。
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）時間範囲を指定します。
time	時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。
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

このコマンドには、デフォルト設定はありません。

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
時間範囲コンフィギュレーション	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

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、セキュリティ アプライアンスのシステム 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、**absolute** キーワードの動作をデフォルトに戻す例を示します。

```
hostname(config-time-range)# default absolute
```

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。
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）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

default-acl

ポスチャ検証が失敗した NAC フレームワーク セッションのデフォルトの ACL として使用されるように ACL を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **default-acl** コマンドを使用します。このコマンドを NAC ポリシーから削除するには、このコマンドの **no** 形式を使用します。

[**no**] **default-acl** *acl-name*

構文の説明

acl-name	セッションに適用されるアクセス コントロール リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

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

使用上のガイドライン

各グループ ポリシーは、ポリシーに一致し、NAC に対して適格なホストに適用されるデフォルト ACL を指しています。セキュリティ アプライアンスは、ポスチャ検証の前に NAC のデフォルト ACL を適用します。ポスチャ検証の後、セキュリティ アプライアンスはデフォルト ACL をリモート ホストのアクセス コントロール サーバから取得した ACL に置き換えます。ポスチャ確認が失敗した場合は、デフォルト ACL がそのまま使われます。

また、セキュリティ アプライアンスは、クライアントレス認証がイネーブルになっている（デフォルト設定）場合にも、NAC のデフォルト ACL を適用します。

例

次に、ポスチャ検証が成功する前に適用される ACL として acl-1 を指定する例を示します。

```
hostname(config-group-policy)# default-acl acl-1
hostname(config-group-policy)
```

次に、デフォルト グループ ポリシーから ACL を継承する例を示します。

```
hostname(config-group-policy)# no default-acl
```

```
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。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
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。

default enrollment

すべての登録パラメータをシステム デフォルト値に戻すには、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 **default enrollment** コマンドを使用します。

default enrollment

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
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、すべての登録パラメータをトラストポイント central 内のデフォルト値に戻す例を示します。

```
hostname<config># crypto ca trustpoint central
hostname<ca-trustpoint># default enrollment
hostname<ca-trustpoint>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crl configure	CRL コンフィギュレーション モードを開始します。
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-domain

グループ ポリシーのユーザのデフォルト ドメイン名を設定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

default-domain {value *domain-name* **| none}**

no default-domain [*domain-name***]**

構文の説明

none	デフォルト ドメイン名がないことを指定します。デフォルト ドメイン名にヌル値を設定して、デフォルト ドメイン名を拒否します。デフォルトまたは指定したグループ ポリシーのデフォルト ドメイン名は継承されません。
value *domain-name*	グループのデフォルト ドメイン名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ユーザがドメイン名を継承しないようにするには、**default-domain none** コマンドを使用します。

セキュリティ アプライアンスは、ドメイン フィールドを省略した DNS クエリーに付加するために、デフォルト ドメイン名を IPSec クライアントに渡します。このドメイン名は、トンネル パケットにのみ適用されます。デフォルト ドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。

デフォルト ドメイン名に使用できるのは、英数字、ハイフン（-）、およびピリオド（.）のみです。

例

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

関連コマンド

コマンド	説明
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。
split-tunnel-policy	IPSec クライアントが条件に応じてパケットを暗号化形式で IPSec トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようにします。

default-group-policy

ユーザがデフォルトで継承する属性のセットを指定するには、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 **default-group-policy** コマンドを使用します。デフォルトのグループ ポリシー名を削除するには、このコマンドの **no** 形式を使用します。

default-group-policy *group-name*

no default-group-policy *group-name*

構文の説明

group-name	デフォルト グループの名前を指定します。

デフォルト

デフォルト グループ名は DfltGrpPolicy です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

バージョン	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 コンフィギュレーション モードの **default-group-policy** コマンドは廃止されました。このコマンドは、トンネル グループ一般属性モードの **default-group-policy** コマンドに置き換えられています。

使用上のガイドライン

バージョン 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 グループ一般属性モードの同等のコマンドに変換されます。

デフォルト グループ ポリシー DfltGrpPolicy には、セキュリティ アプライアンスが初期設定されています。この属性は、すべてのトンネル グループ タイプに適用できます。

例

次に、設定一般コンフィギュレーション モードを開始して、「standard-policy」という名前の IPSec LAN-to-LAN トンネル グループで、ユーザがデフォルトで継承する属性のセットを指定する例を示します。このコマンド セットでは、アカウンティング サーバ、認証サーバ、認可サーバ、およびアドレス プールを定義します。

```
hostname(config)# tunnel-group standard-policy type ipsec-ra
hostname(config)# tunnel-group standard-policy general-attributes
hostname(config-tunnel-general)# default-group-policy first-policy
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)# authorization-server-group aaa-server78
```

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

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
group-policy	グループ ポリシーを作成または編集します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

default-group-policy（webvpn）

WebVPN または電子メール プロキシ設定でグループ ポリシーが指定されない場合に使用するグループ ポリシーの名前を指定するには、さまざまなコンフィギュレーション モードで **default-group-policy** 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。

default-group-policy *groupname*

no default-group-policy

構文の説明

groupname	デフォルト グループ ポリシーとして使用する、設定済みのグループ ポリシーを指定します。**group-policy** コマンドを使用して、グループ ポリシーを設定します。

デフォルト

DfltGrpPolicy という名前のデフォルト グループ ポリシーは、常に、セキュリティ アプライアンスに存在します。この **default-group-policy** コマンドを使用すると、作成したグループ ポリシーを、WebVPN および電子メール プロキシ セッション用のデフォルト グループ ポリシーとして置き換えることができます。または、DfltGrpPolicy を編集することもできます。

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
webvpn コンフィギュレーション	•	—	•	—	—
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—

コマンド履歴

バージョン	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	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、トンネル グループ一般属性コンフィギュレーション モードに移動されました。

使用上のガイドライン

WebVPN セッション、IMAP4S セッション、POP3S セッション、および SMTPS セッションには、指定されたグループ ポリシーまたはデフォルト グループ ポリシーが必要です。WebVPN の場合は、webvpn モードでこのコマンドを使用します。電子メール プロキシの場合、このコマンドは、該当する電子メール プロキシ モードで使用します。

バージョン 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 グループ一般属性モードの同等のコマンドに変換されます。

システムの DefaultGroupPolicy は編集できますが、削除はしないでください。DefaultGroupPolicy の AVP は、次のとおりです。

属性	デフォルト値
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 分
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled
webvpn 属性：	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	none

例

次に、WebVPN7 という名前の WebVPN のデフォルト グループ ポリシーを指定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# default-group-policy WebVPN7
```

default-idle-timeout

WebVPN ユーザのデフォルト アイドル タイムアウト値を設定するには、webvpn コンフィギュレーション モードで **default-idle-timeout** コマンドを使用します。デフォルトのタイムアウト値をコンフィギュレーションから削除し、デフォルトをリセットするには、このコマンドの **no** 形式を使用します。

デフォルト アイドル タイムアウトにより、セッションの失効を回避できます。

default-idle-timeout *seconds*

no default-idle-timeout

構文の説明

seconds	アイドル タイムアウトの秒数を指定します。最小値は 60 秒で、最大値は 1 日（86400 秒）です。

デフォルト

1800 秒（30 分）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

ユーザのアイドル タイムアウトが定義されていない場合、値が 0 の場合、または値が有効な値の範囲外である場合に、セキュリティ アプライアンスでは、ここで設定した値が使用されます。

このコマンドには、短い時間を設定することを推奨します。これは、クッキーをディセーブルにするブラウザ設定（またはプロンプトでクッキーを要求してから拒否するブラウザ設定）によって、ユーザが接続していないにもかかわらずセッション データベースに表示されることがあるためです。許可される最大接続数が 1 に設定されている（**vpn-simultaneous-logins** コマンド）場合、最大接続数がすでに存在することがデータベースによって示されるため、ユーザは再ログインすることができません。アイドル タイムアウトを短く設定すると、このようなファントム セッションを迅速に削除し、ユーザが再ログインできるようにすることができます。

例

次に、デフォルト アイドル タイムアウトを 1200 秒（20 分）に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# default-idle-timeout 1200
```

関連コマンド

コマンド	説明
vpn-simultaneous-logins	許可される同時 VPN セッションの最大数を設定します。グループ ポリシー モードまたはユーザ名モードを使用します。

default-information（EIGRP）

EIGRP ルーティング プロセスのデフォルト ルート情報候補を制御するには、ルータ コンフィギュレーション モードで **default-information** コマンドを使用します。着信更新または発信更新で EIGRP デフォルト ルート情報候補を非表示にするには、このコマンドの **no** 形式を使用します。

default-information {**in** | **out**} [*acl-name*]

no default-information {**in** | **out**}

構文の説明

acl-name	（任意）名前付き標準アクセス リスト。
in	外部のデフォルト ルーティング情報を受け入れるように EIGRP を設定します。
out	外部ルーティング情報をアドバタイズするように EIGRP を設定します。

デフォルト

外部ルートが受け入れられ、送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

アクセス リストが指定されたこのコマンドまたは **default-information** コマンドの **no** 形式のみが実行コンフィギュレーションに表示されます。これは、デフォルト ルーティング情報候補がデフォルトで受け入れられ、送信されるためです。このコマンドの **no** 形式には、*acl-name* 引数はありません。

例

次に、外部デフォルト ルート情報またはデフォルト ルート情報候補の受領をディセーブルにする例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# no default-information in
```

関連コマンド

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

default-information originate（OSPF）

OSPF ルーティング ドメインへのデフォルト外部ルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** 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。

default-information originate [**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *name*]

no default-information originate [[**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *name*]]

構文の説明

always	（任意）ソフトウェアにデフォルト ルートがあるかどうかにかかわらず、常に、デフォルト ルートをアドバタイズします。
metric *value*	（任意）OSPF のデフォルト メトリック値を、0 ～ 16777214 の範囲で指定します。
metric-type {1 | 2}	（任意）OSPF ルーティング ドメインにアドバタイズするデフォルト ルートに関連付けられている外部リンク タイプ 有効な値は、次のとおりです。 • **1**：タイプ 1 の外部ルート • **2**：タイプ 2 の外部ルート
route-map *name*	（任意）適用するルート マップ名。

デフォルト

デフォルト値は次のとおりです。

- **metric** *value* は 1 です。
- **metric-type** は 2 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
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

このコマンドの **no** 形式をオプションのキーワードおよび引数とともに使用すると、コマンドからオプションの情報のみが削除されます。たとえば、**no default-information originate metric** *3* と入力すると、実行コンフィギュレーションのコマンドから **metric** *3* オプションが削除されます。コマンド全体を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式をオプションなしで使用します（**no default-information originate**）。

例

次に、オプションのメトリックおよびメトリック タイプとともに **default-information originate** コマンドを使用する例を示します。

```
hostname(config-router)# default-information originate always metric 3 metric-type 2
hostname(config-router)#
```

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。

default-information originate（RIP）

RIP へのデフォルト ルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** 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。

default-information originate [**route-map** *name*]

no default-information originate [**route-map** *name*]

構文の説明

route-map *name*	（任意）適用するルート マップ名。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

default-information originate コマンドで参照されるルート マップは拡張アクセス リストを使用できません。標準のアクセス リストを使用します。

例

次に、デフォルト ルートを RIP に生成する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# default-information originate
```

関連コマンド

コマンド	説明
router rip	RIP ルーティング プロセスのルータ 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。

default-language

クライアントレス SSL VPN ページに表示されるデフォルト言語を設定するには、webvpn コンフィギュレーション モードで **default-language** コマンドを使用します。

default-language *language*

構文の説明

language	事前にインポート済みの変換テーブル名を指定します。

デフォルト

デフォルト言語は en-us（米国で使用されている英語）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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 アプライアンスでは、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および AnyConnect VPN クライアント ユーザに表示されるユーザ インターフェイスで使用される言語を変換できます。

デフォルト言語は、クライアントレス SSL VPN ユーザがログイン前に、最初にセキュリティ アプライアンスに接続するときに表示されます。その後、トンネル グループ設定またはトンネル ポリシー設定およびこれらの設定が参照するカスタマイズに基づいて言語が表示されます。

例

次に、*Sales* という名前を指定して、デフォルト言語を中国語に変更する例を示します。

```
hostname(config-webvpn)# default-language zh
```

関連コマンド

コマンド	説明
import webvpn translation-table	変換テーブルをインポートします。
revert	キャッシュ メモリから変換テーブルを削除します。
show import webvpn translation-table	インポートした変換テーブルに関する情報を表示します。

default-metric

再配布されるルートの EIGRP メトリックを指定するには、ルータ コンフィギュレーション モードで **default-metric** 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。

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

構文の説明

bandwidth	ルートの最小帯域幅（KB/秒単位）。有効な値は、1 ～ 4294967295 です。
delay	ルート遅延（10 マイクロ秒単位）。有効な値は、1 ～ 4294967295 です。
reliability	正常なパケット伝送の可能性。0 ～ 255 の数値で表されます。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。
loading	ルートの有効な帯域幅。1 ～ 255 の数値で表されます（255 は 100 % のロード）。
mtu	許可する MTU の最小値（バイト単位）。有効な値は 1 ～ 65535 です。

デフォルト

デフォルト メトリックなしで再配布できるのは、接続されているルートのみです。再配布される接続ルートのメトリックは、0 に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

redistribute コマンドで **metric** キーワードおよび属性を使用しない場合は、デフォルト メトリックを使用して、EIGRP にプロトコルを再配布する必要があります。メトリックのデフォルトは、さまざまなネットワークで機能するよう慎重に設定されています。値を変更する場合は、最大限の注意を払うようにしてください。スタティック ルートから再配布する場合のみ、同じメトリックを維持できます。

例

次に、再配布された RIP ルート メトリックが EIGRP メトリックに変換される例を示します。使用する値は、次のとおりです。bandwidth = 1000、delay = 100、reliability = 250、loading = 100、および MTU = 1500。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 172.16.0.0
hostname(config-router)# redistribute rip
hostname(config-router)# default-metric 1000 100 250 100 1500
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成して、そのプロセスのルータ コンフィギュレーション モードを開始します。
redistribute（EIGRP）	EIGRP ルーティング プロセスにルートを再配布します。

delay

インターフェイスの遅延値を設定するには、インターフェイス コンフィギュレーション モードで **delay** コマンドを使用します。デフォルトの遅延値に戻すには、このコマンドの **no** 形式を使用します。

delay *delay-time*

no delay

構文の説明

delay-time	遅延時間（10 マイクロ秒単位）。有効な値は、1 ～ 16777215 です。

デフォルト

デフォルトの遅延はインターフェイス タイプによって異なります。インターフェイスのデフォルト値を確認するには、**show interface** コマンドを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

値は 10 マイクロ秒単位で入力します。**show interface** の出力に表示される遅延値は、マイクロ秒単位です。

例

次に、インターフェイスの遅延をデフォルトの 1000 から 2000 に変更する例を示します。**delay** コマンドの前と後に切り捨てられた **show interface** コマンドの出力が含まれ、このコマンドが遅延値にどのように影響を与えるかを示します。遅延値は、**show interface** の出力の 2 行め、DLY ラベルの後に記載されます。

遅延値を 2000 に変更するために入力するコマンドは、**delay 2000** ではなく **delay 200** です。これは、**delay** コマンドで入力する値が 10 マイクロ秒単位であり、**show interface** の出力ではマイクロ秒単位で表示されるためです。

```
hostname(config)# interface Ethernet0/0
hostname(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed
```

```
hostname(config-if)# delay 200
hostname(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed
```

関連コマンド

コマンド	説明
show interface	インターフェイスの統計情報および設定を表示します。

delete

ディスク パーティションのファイルを削除するには、特権 EXEC モードで **delete** コマンドを使用します。

delete [**/noconfirm**] [**/recursive**] [**flash:**]*filename*

構文の説明

/noconfirm	（任意）確認のためのプロンプトを表示しないように指定します。
/recursive	（任意）すべてのサブディレクトリの指定されたファイルを再帰的に削除します。
filename	削除するファイルの名前を指定します。
flash:	削除できない内部フラッシュを、コロンを付けて指定します。

デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

パスを指定しない場合は、現在の作業ディレクトリからファイルが削除されます。ファイルの削除では、ワイルドカードがサポートされています。ファイルの削除を実行すると、ファイル名のプロンプトが表示されるため、削除を確認する必要があります。

次の例は、現在の作業ディレクトリにある *test.cfg* という名前のファイルを削除する方法を示しています。

```
hostname# delete test.cfg
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
rmdir	ファイルまたはディレクトリを削除します。
show file	指定されたファイルを表示します。

deny-message（グループ ポリシー webvpn コンフィギュレーション モード）

WebVPN に正常にログインした VPN 特権を持たないリモート ユーザに配信されたメッセージを変更するには、グループ webvpn コンフィギュレーション モードで **deny-message value** コマンドを使用します。リモート ユーザがメッセージを受信しないようにストリングを削除するには、このコマンドの **no** 形式を使用します。

deny-message value "*string***"**

no deny-message value

構文の説明

string	491 文字以下の英数字。特殊文字、スペース、および句読点を含みます。

デフォルト

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」

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 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)	このコマンドは、トンネル グループ webvpn コンフィギュレーション モードからグループ webvpn コンフィギュレーション モードに変更されました。

使用上のガイドライン

このコマンドを入力する前に、グローバル コンフィギュレーション モードで **group-policy** *name* **属性** を入力してから、**webvpn** コマンドを入力する必要があります（ポリシー *name* はすでに作成済みと見なされます）。

no deny-message none コマンドは、グループ webvp コンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

deny-message value コマンドへのストリングの入力時は、コマンドがラップしている場合でも引き続き入力します。

VPN セッションに使用されるトンネル ポリシーとは独立して、ログイン時にリモート ユーザのブラウザにテキストが表示されます。

例

次に、group2 という名前の内部グループ ポリシーを作成する最初のコマンドの例を示します。後続のコマンドによって、このポリシーに関連付けられている拒否メッセージを変更します。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
you have not been granted rights to use the VPN features. Contact your administrator for
more information."
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
clear configure group-policy	すべてのグループ ポリシー コンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成します。
group-policy attributes	グループ ポリシー属性コンフィギュレーション モードを開始します。
show running-config group-policy [*name*]	指定したポリシーの実行グループ ポリシー コンフィギュレーションが表示されます。
webvpn（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）	グループ ポリシー webvpn コンフィギュレーション モードを開始します。

deny version

SNMP トラフィックの特定のバージョンを拒否するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。このモードには、グローバル コンフィギュレーション モードから **snmp-map** コマンドを入力してアクセスできます。このコマンド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。

deny version *version*

no deny version *version*

構文の説明

version	セキュリティ アプライアンスがドロップする SNMP トラフィックのバージョンを指定します。使用可能な値は、**1**、**2**、**2c**、および **3** 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
SNMP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

SNMP トラフィックを特定の SNMP バージョンに制限するには、**deny version** コマンドを使用します。以前のバージョンの SNMP はセキュリティがより低いため、セキュリティ ポリシーで SNMP トラフィックを Version 2 に制限できます。**deny version** コマンドは SNMP マップ内で使用します。SNMP マップは、**snmp-map** コマンドを使用して設定します。SNMP マップの作成後に、**inspect snmp** コマンドを使用してこのマップをイネーブルにし、**service-policy** コマンドを使用して 1 つ以上のインターフェイスに適用します。

例

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

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

```
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

description

指定したコンフィギュレーション ユニット（たとえば、コンテキスト、オブジェクト グループ、または DAP レコード）に対する説明を追加するには、各コンフィギュレーション モードで **description** コマンドを使用します。説明により、役立つ情報がコンフィギュレーションに追加されます。説明を削除するには、このコマンドの **no** 形式を使用します。

description *text*

no description

構文の説明

text	説明を最大 200 文字のテキスト ストリングで設定します。ダイナミック アクセス ポリシー レコード モードの場合、最大長は 80 文字です。 ストリングに疑問符（?）を含める場合は、不注意から CLI ヘルプを呼び出さないように、Ctrl+V を入力してから疑問符を入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

このコマンドは、さまざまなコンフィギュレーション モードで使用できます。

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(2)	ダイナミック アクセス ポリシー レコード モードのサポートが追加されました。

例

次に、「管理」コンテキスト コンフィギュレーションに説明を追加する例を示します。

```
hostname(config)# context administrator
hostname(config-context)# description This is the admin context.
hostname(config-context)# allocate-interface gigabitethernet0/0.1
hostname(config-context)# allocate-interface gigabitethernet0/1.1
hostname(config-context)# config-url flash://admin.cfg
```

関連コマンド

コマンド	説明
class-map	**policy-map** コマンドのアクションを適用するトラフィックを指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
gtp-map	GTP インスペクション エンジンのパラメータを制御します。
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。
object-group	**access-list** コマンドに含めるトラフィックを指定します。
policy-map	**class-map** コマンドで指定したトラフィックに適用するアクションを指定します。

dhcp client route distance

DHCP を通じて学習したルートにアドミニストレーティブ ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route distance** 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。

dhcp client route distance *distance*

no dhcp client route distance *distance*

構文の説明

distance	DHCP を通じて学習したルートに適用するアドミニストレーティブ ディスタンス。有効な値は、1 ～ 255 です。

デフォルト

DHCP を通じて学習したルートには、デフォルトでアドミニストレーティブ ディスタンス 1 が指定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

dhcp client route distance コマンドは、ルートが DHCP を通じて学習された場合にのみチェックされます。ルートが DHCP を通じて学習された後に **dhcp client route distance** コマンドが開始されると、指定したアドミニストレーティブ ディスタンスは、学習された既存のルートに影響を与えません。指定したアドミニストレーティブ ディスタンスが設定されるのは、このコマンドの入力後に学習されたルートだけです。

DHCP でルートを取得するには、**ip address dhcp** コマンドで **setroute** オプションを指定する必要があります。

DHCP を複数のインターフェイスで設定している場合、インストールされたルートの優先度を指定するには、各インターフェイスで **dhcp client route distance** コマンドを使用する必要があります。

例

次に、GigabitEthernet0/2 で DHCP によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。SLA 動作が失敗した場合、GigabitEthernet0/3 で DHCP により取得したバックアップ ルートが使用されます。バックアップ ルートには、アドミニストレーティブ ディスタンスに 254 が割り当てられます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

関連コマンド

コマンド	説明
dhcp client route track	DHCP を通じて学習したルートをトラッキング エントリ オブジェクトに関連付けます。
ip address dhcp	指定したインターフェイスに DHCP で取得した IP アドレスを設定します。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

dhcp client route track

追加ルートをトラッキング済みの指定オブジェクト番号に関連付けるように DHCP クライアントを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route track** コマンドを使用します。DHCP クライアントのルート トラッキ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。

dhcp client route track *number*

no dhcp client route track

構文の説明

number	トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 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
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

dhcp client route track コマンドは、ルートが DHCP を通じて学習された場合にのみチェックされます。ルートが DHCP から学習された後で **dhcp client route track** コマンドを入力すると、学習された既存のルートはトラッキング オブジェクトに関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

DHCP でルートを取得するには、**ip address dhcp** コマンドで **setroute** オプションを指定する必要があります。

DHCP を複数のインターフェイスで設定している場合、インストールされたルートの優先度を指定するには、各インターフェイスで **dhcp client route distance** コマンドを使用する必要があります。

例

次に、GigabitEthernet0/2 で DHCP によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。SLA 動作が失敗した場合、GigabitEthernet0/3 で DHCP により取得したバックアップ ルートが使用されます。バックアップ ルートには、アドミニストレーティブ ディスタンスに 254 が割り当てられます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
```

```
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

関連コマンド

コマンド	説明
dhcp client route distance	DHCP を通じて学習したルートにアドミニストレーティブ ディスタンスを割り当てます。
ip address dhcp	指定したインターフェイスに DHCP で取得した IP アドレスを設定します。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

dhcp-client broadcast-flag

セキュリティ アプライアンスによる DHCP クライアント パケットへのブロードキャスト フラグの設定を許可するには、グローバル コンフィギュレーション モードで **dhcp-client broadcast-flag** コマンドを使用します。ブロードキャスト フラグを禁止するには、このコマンドの **no** 形式を使用します。

dhcp-client broadcast-flag

no dhcp-client broadcast-flag

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、ブロードキャスト フラグ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

ip address dhcp コマンドを使用してインターフェイスの DHCP クライアントをイネーブルにすると、DHCP クライアントが検出を送信して IP アドレスを要求するときに、このコマンドを使用して、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定できます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

no dhcp-client broadcast-flag コマンドを入力すると、ブロードキャスト フラグは 0 に設定され、DHCP サーバは応答パケットを提供された IP アドレスのクライアントにユニキャストします。

DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

例

次に、ブロードキャスト フラグをイネーブルにする例を示します。

```
hostname(config)# dhcp-client broadcast-flag
```

関連コマンド

コマンド	説明
ip address dhcp	インターフェイスで DHCP クライアントをイネーブルにします。

interface	IP アドレスを設定するために、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。
dhcp-client client-id	DHCP 要求パケット オプション 61 を、インターフェイス MAC アドレスが含まれるように設定します。
dhcp-client update dns	DHCP クライアントで DNS 更新をイネーブルにします。

dhcp-client client-id

デフォルトの内部生成ストリングではなく、オプション 61 の DHCP 要求パケットに MAC アドレスが保存されるよう強制するには、グローバル コンフィギュレーション モードで **dhcp-client client-id** コマンドを使用します。MAC アドレスを禁止するには、このコマンドの **no** 形式を使用します。

dhcp-client client-id interface *interface_name*

no dhcp-client client-id interface *interface_name*

構文の説明

interface *interface_name*	オプション 61 用に MAC アドレスをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトでは、オプション 61 には内部生成 ASCII ストリングが使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

ip address dhcp コマンドを使用してインターフェイスの DHCP クライアントをイネーブルにすると、一部の ISP でオプション 61 がインターフェイス MAC アドレスであると見なされます。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。**dhcp-client client-id** コマンドを使用して、オプション 61 用にインターフェイス MAC アドレスを含めます。

例

次に、外部インターフェイスのオプション 61 用に MAC アドレスをイネーブルに例を示します。

```
hostname(config)# dhcp-client client-id interface outside
```

関連コマンド

コマンド	説明
ip address dhcp	インターフェイスで DHCP クライアントをイネーブルにします。
interface	IP アドレスを設定するために、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。

dhcp-client broadcast-flag	DHCP クライアント パケットにブロードキャスト フラグを設定します。
dhcp-client update dns	DHCP クライアントで DNS 更新をイネーブルにします。

dhcp-client update dns

DHCP クライアントが DHCP サーバに渡す更新パラメータを設定するには、グローバル コンフィギュレーション モードで **dhcp-client update dns** コマンドを使用します。DHCP クライアントが DHCP サーバに渡すパラメ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。

dhcp-client update dns [**server** {**both** | **none**}]

no dhcp-client update dns [**server** {**both** | **none**}]

構文の説明

both	DHCP サーバが DNS A および PTR リソース レコードの両方を更新するクライアント要求。
none	DHCP サーバが DDNS 更新を実行しないクライアント要求。
server	DHCP サーバがクライアント要求を受信するように指定します。

デフォルト

デフォルトでは、セキュリティ アプライアンスは、DHCP サーバが PTR RR 更新のみを実行するよう要求します。クライアントはサーバに FQDN オプションを送信しません。

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
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドはインターフェイス コンフィギュレーション モードでも入力できますが、ハイフンは使用しません。「**dhcp client update dns**」を参照してください。インターフェイス モードで **dhcp client update dns** コマンドを入力すると、グローバル コンフィギュレーション モードのこのコマンドで設定した設定値が上書きされます。

例

次に、DHCP サーバが A および PTR RR を更新しないことを要求するようクライアントを設定する例を示します。

```
hostname(config)# dhcp-client update dns server none
```

次に、サーバが A および PTR RR を更新することを要求するようクライアントを設定する例を示します。

```
hostname(config)# dhcp-client update dns server both
```

関連コマンド

コマンド	説明
ddns（DDNS 更新方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	Dynamic DNS（DDNS; ダイナミック DNS）アップデート方式を、セキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp client update dns	
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcp-network-scope

セキュリティ アプライアンス DHCP サーバが、このグループ ポリシーのユーザにアドレスを割り当てるために使用する必要がある IP アドレスの範囲を指定するには、グループ ポリシー コンフィギュレーション モードで **dhcp-network-scope** 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。値を継承できないようにするには、**dhcp-network-scope none** コマンドを使用します。

dhcp-network-scope {*ip_address*} | none

no dhcp-network-scope

構文の説明

ip_address	このポリシー グループのユーザに IP アドレスを割り当てるため、DHCP サーバが使用する必要がある IP サブネットワークを指定します。
none	DHCP サブネットワークをヌル値に設定して、IP アドレスが許可されないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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、First Group という名前のグループ ポリシーに対して、IP サブネットワーク 10.10.85.0 を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

dhcp-server

VPN トンネルの確立時にクライアントに IP アドレスを割り当てる DHCP サーバのサポートを設定するには、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 **dhcp-server** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

dhcp-server [link-selection | subnet-selection] <ip1> [<ip2>...<ip10>]

[no] dhcp-server [link-selection | subnet-selection] <ip1> [<ip2>...<ip10>]

構文の説明

<ip1>	DHCP サーバのアドレス。
<ip2>-<ip10>	（任意）追加の DHCP サーバ。 1 回のコマンドで最大 10 個まで指定できます。また、複数のコマンドにまたがって指定できます。
link-selection	（任意）セキュリティ アプライアンスが RFC 3527 で定義されている DHCP サブ オプション 5（リレー情報オプション 82 のリンク選択のサブオプション）を送信するかどうかを指定するための設定。この設定は、この RFC をサポートするサーバでのみ使用してください。
subnet-selection	（任意）セキュリティ アプライアンスが RFC 3011 で定義されている DHCP オプション 118（IPv4 サブネットの選択のオプション）を送信するかどうかを指定するための設定。この設定は、この RFC をサポートするサーバでのみ使用してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(5)	link-selection オプションおよび subnet-selection オプションを追加しました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル グループ タイプに対してのみ適用できます。

例

次のコマンドを config-general コンフィギュレーション モードで入力して、3 つの DHCP サーバ（dhcp1、dhcp2、および dhcp3）を IPSec リモートアクセス トンネル グループ「remotegrp」に追加する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
hostname(config-tunnel-general)
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

dhcpd address

DHCP サーバで使用される IP アドレス プールを定義するには、グローバル コンフィギュレーション モードで **dhcpd address** コマンドを使用します。既存の DHCP アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

dhcpd address *IP_address1*[-*IP_address2*] *interface_name*

no dhcpd address *interface_name*

（注） プールのサイズは、Cisco ASA 5505 のユーザ ライセンス数が 10 の場合は 32 アドレス、Cisco ASA 5505 のユーザ ライセンス数が 50 の場合は 128 アドレスにそれぞれ制限されます。Cisco ASA 5505 のユーザ ライセンスが無制限の場合、およびその他すべてのセキュリティ アプライアンス プラットフォーム上では、256 アドレスがサポートされます。

構文の説明

interface_name	アドレス プールの割り当て先のインターフェイス。
IP_address1	DHCP アドレス プールの開始アドレス。
IP_address2	DHCP アドレス プールの終了アドレス。

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
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

dhcpd address *ip1*[-*ip2*] *interface_name* コマンドは、DHCP サーバのアドレス プールを指定します。セキュリティ アプライアンス DHCP サーバのアドレス プールは、そのアドレス プールがイネーブルなセキュリティ アプライアンス インターフェイスと同じサブネット内にある必要があります。また、*interface_name* を使用して関連するセキュリティ アプライアンス インターフェイスを指定する必要があります。

アドレス プールのサイズは、セキュリティ アプライアンスでプールあたり 256 に制限されています。アドレス プールの範囲が 253 アドレスよりも大きい場合、セキュリティ アプライアンス インターフェイスのネットマスクは、クラス C アドレス（たとえば、255.255.255.0）にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

DHCP クライアントは、物理的にセキュリティ アプライアンス DHCP サーバ インターフェイスのサブネットに接続されている必要があります。

dhcpd address コマンドでは、「-」（ダッシュ）文字がオブジェクト名の一部ではなく、範囲指定子と解釈されるため、「-」文字を含むインターフェイス名は使用できません。

no dhcpd address *interface_name* コマンドは、指定されたインターフェイスに設定されている DHCP サーバ アドレス プールを削除します。

DHCP サーバ機能をセキュリティ アプライアンスに実装する方法については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

次に、**dhcpd address** コマンド、**dhcpd dns** コマンド、および **dhcpd enable** *interface_name* コマンドを使用して、セキュリティ アプライアンスの **dmz** インターフェイスに DHCP クライアントに対するアドレス プールおよび DNS サーバを設定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 209.165.200.226
hostname(config)# dhcpd enable dmz
```

次に、内部インターフェイスに DHCP サーバを設定する例を示します。その内部インターフェイスの DHCP サーバに IP アドレス 10 個のプールを割り当てるため、**dhcpd address** コマンドを使用します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd auto_config

DHCP または PPPoE クライアントを実行しているインターフェイスから取得した値に基づいて、セキュリティ アプライアンスが DHCP サーバに対して DNS、WINS およびドメイン名の値を自動的に設定するの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 **dhcpd auto_config** コマンドを使用します。DHCP パラメータの自動設定を解除するには、このコマンドの **no** 形式を使用します。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

構文の説明

client_if_name	DNS、WINS、およびドメイン名パラメータを提供する DHCP クライアントを実行している、インターフェイスを指定します。
interface *if_name*	アクションが適用されるインターフェイスを指定します。
vpnclient-wins-override	vpnclient パラメータにより、インターフェイス DHCP または PPPoE クライアントの WINS パラメータを上書きします。

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

CLI コマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定によって取得されたパラメータは、CLI により設定されたパラメータで上書きされます。

例

次に、内部インターフェイスに DHCP を設定する例を示します。外部インターフェイス上の DHCP クライアントから取得した DNS、WINS、およびドメイン情報を、内部インターフェイス上の DHCP クライアントに渡すには、**dhcpd auto_config** コマンドを使用します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd auto_config outside
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show ip address dhcp server	DHCP クライアントとして動作するインターフェイスに DHCP サーバから提供される、DHCP オプションに関する詳細情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd dns

DHCP クライアントに対して DNS サーバを定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。定義されたサーバをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

no dhcpd dns [*dnsip1* [*dnsip2*]] [**interface** *if_name*]

構文の説明

dnsip1	DHCP クライアントに対するプライマリ DNS サーバの IP アドレス。
dnsip2	（任意）DHCP クライアントの代替 DNS サーバの IP アドレス。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

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
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

dhcpd dns コマンドは、DHCP クライアントに対する DNS サーバの IP アドレスを 1 つまたは複数指定します。2 つの DNS サーバを指定できます。**no dhcpd dns** コマンドは、コンフィギュレーションから DNS IP アドレスを削除します。

例

次に、**dhcpd address** コマンド、**dhcpd dns** コマンド、および **dhcpd enable** *interface_name* コマンドを使用して、セキュリティ アプライアンスの **dmz** インターフェイスに DHCP クライアントに対するアドレス プールおよび DNS サーバを設定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 192.168.1.2
hostname(config)# dhcpd enable dmz
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
dhcpd wins	DHCP クライアントに対して WINS サーバを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd domain

DHCP クライアントに対して DNS ドメイン名を定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。DNS ドメイン名をクリアするには、このコマンドの **no** 形式を使用します。

dhcpd domain *domain_name* [**interface** *if_name*]

no dhcpd domain [*domain_name*] [**interface** *if_name*]

構文の説明

domain_name	example.com などの DNS ドメイン名。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

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
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

dhcpd domain コマンドは、DHCP クライアントに対する DNS ドメイン名を指定します。**no dhcpd domain** コマンドは、コンフィギュレーションから DNS ドメイン サーバを削除します。

例

次に、**dhcpd domain** コマンドを使用して、セキュリティ アプライアンスで DHCP サーバにより DHCP クライアントに提供されるドメイン名を設定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd enable

DHCP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd enable** コマンドを使用します。DHCP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。DHCP サーバは、DHCP クライアントにネットワーク コンフィギュレーション パラメータを提供します。セキュリティ アプライアンス内で DHCP サーバをサポートすることにより、セキュリティ アプライアンスは DHCP を使用して接続されるクライアントを設定できるようになります。

dhcpd enable *interface*

no dhcpd enable *interface*

構文の説明

interface	DHCP サーバをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、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

dhcpd enable *interface* コマンドを使用すると、DHCP デーモンによる、DHCP 対応のインターフェイス上での DHCP クライアントの要求のリッスンをイネーブルにできます。**no dhcpd enable** コマンドは、指定したインターフェイス上の DHCP サーバ機能をディセーブルにします。

（注） マルチ コンテキスト モードの場合は、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP サーバをイネーブルにすることはできません。

セキュリティ アプライアンスが DHCP クライアント要求に応答する場合、要求を受信したインターフェイスの IP アドレスとサブネット マスクを、デフォルト ゲートウェイの IP アドレスとサブネット マスクとして応答で使用します。

（注） セキュリティ アプライアンス DHCP サーバ デーモンは、直接セキュリティ アプライアンス インターフェイスに接続されていないクライアントはサポートしません。

DHCP サーバ機能をセキュリティ アプライアンスに実装する方法については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

次に、**dhcpd enable** コマンドを使用して、DHCP サーバを内部インターフェイス上でイネーブルにする例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
debug dhcpd	DHCP サーバのデバッグ情報を表示します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd lease

DHCP リース期間を指定するには、グローバル コンフィギュレーション モードで **dhcpd lease** コマンドを使用します。リースの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。

dhcpd lease *lease_length* [**interface** *if_name*]

no dhcpd lease [*lease_length*] [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
lease_length	DHCP サーバから DHCP クライアントに与えられる、秒単位の IP アドレスのリース期間。有効な値は、300 ～ 1048575 秒です。

デフォルト

lease_length のデフォルト値は 3600 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

dhcpd lease コマンドは、DHCP クライアントに与えるリース期間を秒単位で指定します。このリース期間は、DHCP サーバが割り当てた IP アドレスを DHCP クライアントが使用できる期間を示します。

no dhcpd lease コマンドは、コンフィギュレーションから指定したリース期間を削除して、この値をデフォルト値の 3600 秒に置き換えます。

例

次に、**dhcpd lease** コマンドを使用して、DHCP クライアントに対する DHCP 情報のリース期間を指定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd option

DHCP オプションを設定するには、グローバル コンフィギュレーション モードで **dhcpd option** コマンドを使用します。オプションをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd option *code* {**ascii** *string*} | {**ip** *IP_address* [*IP_address*]} | {**hex** *hex_string*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

構文の説明

ascii	オプション パラメータが ASCII 文字ストリングであることを指定します。
code	設定された DHCP オプションの番号。有効な値は、0 ～ 255 であり、いくつかの例外があります。サポートされていない DHCP オプション コードのリストについては、下の使用上のガイドラインを参照してください。
hex	オプション パラメータが 16 進ストリングであることを指定します。
hex_string	16 進ストリングをスペースのない偶数桁で指定します。0x プレフィックスを使用する必要はありません。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
ip	オプション パラメータが IP アドレスであることを指定します。最大 2 つの IP アドレスを **ip** キーワードに指定できます。
IP_address	ドット付き 10 進表記の IP アドレスを指定します。
string	スペースなしの ASCII 文字ストリングを指定します。

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です。

使用上のガイドライン

dhcpd option コマンドを使用して、TFTP サーバ情報を Cisco IP Phone およびルータに提供することができます。

DHCP オプション要求がセキュリティ アプライアンス DHCP サーバに到着すると、セキュリティ アプライアンスは **dhcpd option** コマンドで指定された値を、クライアントに対する応答に入れます。

dhcpd option 66 コマンドおよび **dhcpd option 150** コマンドは、Cisco IP Phone およびルータがコンフィギュレーション ファイルをダウンロードするときに使用する TFTP サーバを指定します。次のようにコマンドを使用します。

- **dhcpd option 66 ascii** *string*。ここで、*string* は TFTP サーバの IP アドレスまたはホスト名です。オプション 66 には、TFTP サーバを 1 つだけ指定できます。
- **dhcpd option 150 ip** *IP_address* [*IP_address*]。ここで、*IP_address* は TFTP サーバの IP アドレスです。オプション 150 には、最大 2 つの IP アドレスを指定できます。

（注）　**dhcpd option 66** コマンドは **ascii** パラメータのみ受け付け、**dhcpd option 150** コマンドは **ip** パラメータのみ受け付けます。

dhcpd option 66 | 150 コマンドに IP アドレスを指定するときには、次のガイドラインに従ってください。

- TFTP サーバが DHCP サーバ インターフェイス上にある場合、TFTP サーバのローカル IP アドレスを使用します。
- TFTP サーバが DHCP サーバ インターフェイスよりもセキュリティが低いインターフェイス上にある場合は、一般の発信ルールが適用されます。DHCP クライアント用の NAT エントリ、グローバル エントリ、および **access-list** エントリを作成し、TFTP サーバの実際の IP アドレスを使用します。
- TFTP サーバがよりセキュリティの高いインターフェイス上にある場合は、一般の着信ルールが適用されます。TFTP サーバ用のスタティック ステートメントと **access-list** ステートメントのグループを作成し、TFTP サーバのグローバル IP アドレスを使用します。

その他の DHCP オプションの詳細については、RFC2132 を参照してください。

（注）　セキュリティ アプライアンスは、与えられたオプション タイプおよび値が RFC 2132 に規定されているオプション コードの想定タイプおよび想定値と一致していることを確認しません。たとえば、**dhcpd option 46 ascii hello** と入力した場合、セキュリティ アプライアンスはその設定を受け入れますが、オプション 46 は 1 桁の 16 進値が想定されるとして RFC 2132 に規定されます。

dhcpd option コマンドで次の DHCP オプションは設定できません。

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER

オプション コード	説明
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

例

次に、DHCP オプション 66 に TFTP サーバを指定する例を示します。

```
hostname(config)# dhcpd option 66 ascii MyTftpServer
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd ping_timeout

DHCP ping のデフォルト タイムアウトを変更するには、グローバル コンフィギュレーション モードで **dhcpd ping_timeout** 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。アドレスの競合を避けるため、DHCP サーバは、アドレスを DHCP クライアントに割り当てる前に 2 つの ICMP ping パケットをアドレスに送信します。このコマンドは、ping タイムアウトをミリ秒で指定します。

dhcpd ping_timeout *number* [**interface** *if_name*]

no dhcpd ping_timeout [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
number	ミリ秒単位の ping タイムアウト値。最小値は 10、最大値は 10000 です。デフォルト値は 50 です。

デフォルト

number のデフォルトのミリ秒は 50 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスは、DHCP クライアントに IP アドレスを割り当てる前に、両方の ICMP ping パケットがタイムアウトになるのを待ちます。たとえば、デフォルト値が使用された場合、セキュリティ アプライアンスは IP アドレスを割り当てる前に、1500 ミリ秒（各 ICMP ping パケットに対して 750 ミリ秒）待ちます。

ping のタイムアウト値が長いと、DHCP サーバのパフォーマンスに悪影響を及ぼす場合があります。

例

次に、**dhcpd ping_timeout** コマンドを使用して、DHCP サーバの ping タイムアウト値を変更する例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
```

```
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd update dns

DHCP サーバによるダイナミック DNS 更新の実行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 **dhcpd update dns** コマンドを使用します。DHCP サーバによる DDNS 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。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

構文の説明

both	DHCP サーバが A と PTR の両方の DNS RR を更新するように指定します。
interface	DDNS 更新が適用されるセキュリティ アプライアンス インターフェイスを指定します。
override	DHCP サーバが DHCP クライアント要求を上書きするように指定します。
srv_ifc_name	このオプションを適用するインターフェイスを指定します。

デフォルト

デフォルトでは、DHCP サーバは PTR RR 更新のみを実行します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。更新は DHCP サーバと連携して実行されます。**dhcpd update dns** コマンドはサーバによる更新をイネーブルにします。

名前とアドレスのマッピングは、次の 2 タイプの RR に保持されます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

dhcpd update dns コマンドを使用すると、DHCP サーバが A RR と PRT RR の両方の更新、または PTR RR 更新のみを実行するように設定できます。DHCP クライアントからの更新要求を上書きするように設定することもできます。

例

次に、DDNS サーバが DHCP クライアントからの要求を上書きすると同時に、A と PTR の両方の更新を実行するよう設定する例を示します。

```
hostname(config)# dhcpd update dns both override
```

関連コマンド

コマンド	説明
ddns（DDNS 更新方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	DDNS アップデート方式をセキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcpd wins

DHCP クライアントに対して WINS サーバを定義するには、グローバル コンフィギュレーション モードで **dhcpd wins** コマンドを使用します。WINS サーバを DHCP サーバから削除するには、このコマンドの **no** 形式を使用します。

dhcpd wins *server1* [*server2*] [**interface** *if_name*]

no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
server1	プライマリの Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。
server2	（任意）代替の Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

dhcpd wins コマンドは、DHCP クライアント用の WINS サーバのアドレスを指定します。**no dhcpd wins** コマンドは、コンフィギュレーションから WINS サーバの IP アドレスを削除します。

例

次に、dhcpd wins コマンドを使用して、DHCP クライアントに送信された WINS サーバ情報を指定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd dns	DHCP クライアントに対して DNS サーバを定義します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcprelay enable

DHCP リレー エージェント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 **dhcprelay enable** コマンドを使用します。DHCP リレー エージェント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。DHCP リレー エージェントでは、指定したセキュリティ アプライアンス インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

構文の説明

interface_name	DHCP リレー エージェントがクライアント要求を受け入れるインターフェイスの名前。

デフォルト

DHCP リレー エージェント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
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスが **dhcprelay enable** *interface_name* コマンドを使用して DHCP リレー エージェントを開始するには、**dhcprelay server** コマンドがコンフィギュレーションにすでに存在している必要があります。このコマンドがない場合、セキュリティ アプライアンスは次に示すようなエラー メッセージを表示します。

```
DHCPRA: Warning - There are no DHCP servers configured!
       No relaying can be done without a server!
       Use the 'dhcprelay server <server_ip> <server_interface>' command
```

次の条件下では、DHCP リレーをイネーブルにできません。

- 同じインターフェイス上で DHCP リレーと DHCP リレー サーバをイネーブルにすることはできません。
- 同じインターフェイス上で DHCP リレーと DHCP サーバ（**dhcpd enable**）をイネーブルにすることはできません。
- 1 つのコンテキスト上で、DHCP リレーを DHCP サーバと同時にイネーブルにすることはできません。

- マルチ コンテキスト モードの場合、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP リレーをイネーブルにすることはできません。

no dhcprelay enable *interface_name* コマンドは、*interface_name* で指定されたインターフェイスの DHCP リレー エージェント コンフィギュレーションだけを削除します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイスに設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

次に、DHCP リレー エージェントをディセーブルにする例を示します。

```
hostname(config)# no dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcp relay	DHCP リレー エージェントのデバッグ情報を表示します。
dhcprelay server	DHCP リレー エージェントが DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay server

DHCP 要求が転送される DHCP サーバを指定するには、グローバル コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。DHCP サーバを DHCP リレー 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。DHCP リレー エージェントでは、指定したセキュリティ アプライアンス インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

dhcprelay server *IP_address interface_name*

no dhcprelay server *IP_address* [*interface_name*]

構文の説明

interface_name	DHCP サーバが常駐するセキュリティ アプライアンス インターフェイスの名前。
IP_address	DHCP リレー エージェントがクライアント DHCP 要求を転送する DHCP サーバの 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
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

インターフェイスあたり最大 4 つの DHCP リレー サーバを追加できますが、セキュリティ アプライアンスに設定できる DHCP リレー サーバは 10 までという制限があります。**dhcprelay enable** コマンドを入力する前に、少なくとも 1 つの **dhcprelay server** コマンドをセキュリティ アプライアンス コンフィギュレーションに追加する必要があります。DHCP リレー サーバが設定されているインターフェイス上には、DHCP クライアントを設定できません。

dhcprelay server コマンドは、指定したインターフェイス上で UDP ポート 67 を開き、**dhcprelay enable** コマンドがコンフィギュレーションに追加されるとすぐに DHCP リレー タスクを開始します。

no dhcprelay server *IP_address* [*interface_name*] コマンドを使用すると、インターフェイスは DHCP パケットのそのサーバへの転送を停止します。

no dhcprelay server *IP_address* [*interface_name*] コマンドを使用すると、*IP_address* [*interface_name*] で指定された DHCP サーバ用の DHCP リレー エージェント コンフィギュレーションだけが削除されます。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイスに設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay setroute

DHCP 応答にデフォルト ゲートウェイ アドレスを設定するには、グローバル コンフィギュレーション モードで **dhcprelay setroute** コマンドを使用します。デフォルト 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。このコマンドを使用すると、DHCP 応答のデフォルト IP アドレスは、指定されたセキュリティ アプライアンス インターフェイスのアドレスに置き換えられます。

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

構文の説明

interface	最初のデフォルト IP アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように DHCP リレー エージェントを設定します。

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

dhcprelay setroute *interface* コマンドを使用すると、DHCP リレー エージェントが最初のデフォルト ルータ アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように設定できます。

パケット内にデフォルトのルータ オプションがない場合、セキュリティ アプライアンスは *interface* アドレスを含むデフォルト ルータを追加します。その結果、クライアントは自分のデフォルト ルートがセキュリティ アプライアンスに向かうように設定できます。

dhcprelay setroute *interface* コマンドを設定しない場合（かつパケット内にデフォルトのルータ オプションがある場合）、パケットは、ルータ アドレスが変更されないままセキュリティ アプライアンスを通過します。

例

次に、**dhcprelay setroute** コマンドを使用して、DHCP 応答のデフォルト ゲートウェイを外部 DHCP サーバからセキュリティ アプライアンスの内部インターフェイスに設定する例を示します。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
```

```
hostname(config)# dhcprelay setroute inside
hostname(config)# dhcprelay enable inside
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay timeout

DHCP リレー エージェントのタイムアウト値を設定するには、グローバル コンフィギュレーション モードで **dhcprelay timeout** コマンドを使用します。タイムアウト値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。

dhcprelay timeout *seconds*

no dhcprelay timeout

構文の説明

seconds	DHCP リレー アドレス ネゴシエーション用に許可されている時間（秒）を指定します。

デフォルト

dhcprelay タイムアウトのデフォルト値は 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	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

dhcprelay timeout コマンドは、DHCP サーバからの応答がリレー バインディング構造を通して DHCP クライアントに進むことが許されている時間を秒単位で設定します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイスに設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dialog

WebVPN ユーザに表示するダイアログ メッセ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 **dialog** 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。

dialog {**title** | **message** | **border**} **style** *value*

no dialog {**title** | **message** | **border**} **style** *value*

構文の説明

border	境界を変更することを指定します。
message	メッセージ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。
title	タイト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 CSS パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのスタイルは background-color:#669999;color:white です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:black です。

デフォルトの境界線のスタイルは border:1px solid black;border-collapse:collapse です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn カスタマイゼーション 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

style オプションは、任意の有効な 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 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、ダイアログ メッセージの文字表示色を青色に変更するようにカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# dialog message style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

dir

ディレクトリの内容を表示するには、特権 EXEC モードで **dir** コマンドを使用します。

dir [/all] [**all-filesystems**] [**/recursive**] [**flash:** | **system:**] [*path]*

構文の説明

/all	（任意）すべてのファイルを表示します。
all-filesystems	（任意）すべてのファイルシステムのファイルを表示します。
disk0:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
/recursive	（任意）ディレクトリの内容を再帰的に表示します。
system:	（任意）ファイル システムのディレクトリの内容を表示します。
flash:	（任意）デフォルトのフラッシュ パーティションのディレクトリ内容を表示します。
path	（任意）特定のパスを指定します。

デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
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

キーワードまたは引数のない **dir** コマンドは、現在のディレクトリの内容を表示します。

例

次に、ディレクトリの内容を表示する例を示します。

```
hostname# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次に、ファイル システム全体の内容を再帰的に表示する例を示します。

```
hostname# dir /recursive disk0:
Directory of disk0:/*
```

```
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。
mkdir	ディレクトリを作成します。
rmdir	ディレクトリを削除します。

disable

特権 EXEC モードを終了してユーザ EXEC モードに戻るには、特権 EXEC モードで **disable** コマンドを使用します。

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

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

enable コマンドを使用して、特権モードを開始します。**disable** コマンドは、特権モードを終了して、ユーザ モードに戻ります。

例

次の例は、特権モードを開始する方法を示しています。

```
hostname> enable
hostname#
```

次に、特権モードを終了する例を示します。

```
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードをイネーブルにします。

disable（キャッシュ）

WebVPN に対するキャッシングをディセーブルにするには、キャッシュ コンフィギュレーション モードで **disable** コマンドを使用します。キャッシングを再度イネーブルにするには、このコマンドの **no** 形式を使用します。

disable

no disable

デフォルト

キャッシングは、各キャッシュ属性に対するデフォルトの設定でイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

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

キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮したりする必要性を減らすことができます。キャッシングにより、WebVPN とリモート サーバおよびエンド ユーザのブラウザの両方の間のトラフィックが削減されて、多くのアプリケーションの実行効率が大幅に向上されます。

例

次に、キャッシングをディセーブルにしてから、それを再度イネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# disable
hostname(config-webvpn-cache)# no disable
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。

コマンド	説明
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

disable service-settings

電話プロキシ機能の使用時に IP 電話のサービス設定をディセーブルにするには、電話プロキシ コンフィギュレーション モードで **disable service-settings** コマンドを使用します。IP 電話の設定を保持するには、このコマンドの **no** 形式を使用します。

disable service-settings

no disable service-settings

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

サービス設定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	透過	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、次の設定内容が IP 電話ではディセーブルになります。

- PC ポート
- Gratuitous ARP
- Voice VLAN アクセス
- Web アクセス
- Span to PC Port

設定されている各 IP フォンの CUCM で設定されている設定を保持するには、**no disable service-settings** コマンドを設定します。

例

次に、**disable service-settings** コマンドを使用して、ASA で電話プロキシ機能を使用する IP 電話の設定を保持する例を示します。

```
hostname(config-phone-proxy)# no disable service-settings
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
show phone-proxy	Phone Proxy 固有の情報を表示します。

display

セキュリティ アプライアンスが DAP 属性データベースに書き込む属性値のペアを表示するには、DAP テスト属性モードで **display** コマンドを入力します。

display

コマンド デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

通常、セキュリティ アプライアンスは AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。セキュリティ アプライアンスは、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。**display** コマンドを使用すると、これらの属性をコンソールに表示できます。

関連コマンド

コマンド	説明
attributes	属性モードを開始します。このモードでは属性値のペアを設定できます。
dynamic-access-policy-record	DAP レコードを作成します。
test dynamic-access-policy attributes	属性サブモードを開始します。
test dynamic-access-policy execute	DAP を生成するロジックを実行し、生成されたアクセス ポリシーをコンソールに表示します。

distance eigrp

内部および外部 EIGRP ルートのアドミニストレーティブ ディスタンスを設定するには、ルータ コンフィギュレーション モードで **distance eigrp** 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。

distance eigrp *internal-distance external-distance*

no distance eigrp

構文の説明

external-distance	EIGRP 外部ルートのアドミニストレーティブ ディスタンス。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効な値は、1 ～ 255 です。
internal-distance	EIGRP 内部ルートのアドミニストレーティブ ディスタンス。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効な値は、1 ～ 255 です。

デフォルト

デフォルト値は次のとおりです。

- *external-distance* は 170 です。
- *internal-distance* は 90 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
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

各ルーティング プロトコルには、他のルーティング プロトコルと異なるアルゴリズムに基づいたメトリックがあるため、異なるルーティング プロトコルによって生成された同じ宛先への 2 つのルートのいずれが「最適パス」であるかは、必ずしも判別できません。アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先に複数の異なるルートがある場合に、セキュリティ アプライアンスが最適なパスの選択に使用するルート パラメータです。

セキュリティ アプライアンスで複数のルーティング プロトコルが実行されている場合、**distance eigrp** コマンドを使用して、EIGRP ルーティング プロトコルが検出するルートのデフォルト アドミニストレーティブ ディスタンスを、他のルーティング プロトコルと関連付けて調整できます。表 11-1 に、セキュリティ アプライアンスでサポートされているルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンスを示します。

表 11-1　デフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
EIGRP 集約ルート	5
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
不明	255

このコマンドの **no** 形式はキーワードまたは引数を使用しません。コマンドの **no** 形式を使用すると、内部と外部の両方の EIGRP ルートのアドミニストレーティブ ディスタンスがデフォルトに戻されます。

例

次に、**distance eigrp** コマンドを使用して、すべての EIGRP 内部ルートのアドミニストレーティブ ディスタンスを 80 に、すべての EIGRP 外部ルートのアドミニストレーティブ ディスタンスを 115 に設定する例を示します。EIGRP 外部ルートのアドミニストレーティブ ディスタンスを 115 に設定すると、EIGRP によって検出されたルートが、RIP（OSPF ではなく）によって検出された同じルートを経由する特定の宛先設定に渡されます。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 192.168.7.0
hostname(config-router)# network 172.16.0.0
hostname(config-router)# distance eigrp 90 115
```

関連コマンド

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

distance ospf

ルート タイプに基づいて OSPF ルートのアドミニストレーティブ ディスタンスを定義するには、ルータ コンフィギュレーション モードで **distance ospf** 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。

distance ospf [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]

no distance ospf

構文の説明

d1、*d2*、*d3*	各ルート タイプの距離。有効値の範囲は、1 ～ 255 です。
external	（任意）再配布によって取得した他のルーティング ドメインからのルートに距離を設定します。
inter-area	（任意）あるエリアから別のエリアまでのルートすべての距離を設定します。
intra-area	（任意）あるエリア内のすべてのルートの距離を設定します。

デフォルト

d1、*d2*、および *d3* のデフォルト値は 110 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
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

少なくとも 1 つのキーワードと引数を指定する必要があります。アドミニストレーティブ ディスタンスのタイプごとにコマンドを個別に入力することができますが、コンフィギュレーションでは 1 つのコマンドとして表示されます。アドミニストレーティブ ディスタンスを再入力する場合、対象ルート タイプのアドミニストレーティブ ディスタンスだけが変更されます。その他のルート タイプのアドミニストレーティブ ディスタンスは影響されません。

このコマンドの **no** 形式はキーワードまたは引数を使用しません。コマンドの **no** 形式を使用すると、すべてのルート タイプのアドミニストレーティブ ディスタンスがデフォルトに戻されます。複数のルート タイプを設定している場合、1 つのルート タイプをデフォルトのアドミニストレーティブ ディスタンスに戻すには、次のいずれかを実行します。

- ルート タイプを、手動でデフォルト値に設定します。
- コマンドの **no** 形式を使用してコンフィギュレーション全体を削除してから、保持するルート タイプのコンフィギュレーションを再入力します。

例

次に、外部ルートのアドミニストレーティブ ディスタンスを 150 に設定する例を示します。

```
hostname(config-router)# distance ospf external 105
hostname(config-router)#
```

次に、各ルート タイプに入力した個別のコマンドが、ルータ コンフィギュレーションで 1 つのコマンドとして表示される例を示します。

```
hostname(config-router)# distance ospf intra-area 105 inter-area 105
hostname(config-router)# distance ospf intra-area 105
hostname(config-router)# distance ospf external 105
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
hostname(config)#
```

次に、各アドミニストレーティブ ディスタンスを 105 に設定し、次に外部アドミニストレーティブ ディスタンスのみを 150 に変更する例を示します。**show running-config router ospf** コマンドは、外部ルート タイプの値だけが変更され、その他のルート タイプでは以前に設定された値が保持されている状況を示します。

```
hostname(config-router)# distance ospf external 105 intra-area 105 inter-area 105
hostname(config-router)# distance ospf external 150
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
hostname(config)#
```

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。

distribute-list in

ルーティング アップデートで受信するネットワークをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list in** 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。

distribute-list *acl* **in** [**interface** *if_name*]

no distribute-list *acl* **in** [**interface** *if_name*]

構文の説明

acl	標準アクセス リスト名。
if_name	（任意）**nameif** コマンドで指定したインターフェイス名。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスで受信されたルーティング アップデートにのみ適用されます。

デフォルト

着信更新の場合、ネットワークはフィルタリングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

インターフェイスが指定されていない場合、アクセス リストはすべての着信更新に適用されます。

例

次に、外部インターフェイスで受信する RIP ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
hostname(config)# access-list ripfilter permit 10.0.0.0
hostname(config)# access-list ripfilter deny any
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter in interface outside
```

次に、外部インターフェイスで受信する EIGRP ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
hostname(config)# access-list eigrp_filter permit 10.0.0.0
hostname(config)# access-list eigrp_filter deny any
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
```

```
hostname(config-router)# distribute-list eigrp_filter in interface outside
```

関連コマンド

コマンド	説明
distribute-list out	ルーティング アップデートでアドバタイズされるネットワークをフィルタリングします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスのルータ 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。

distribute-list out

ルーティング アップデートで送信される特定のネットワークをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list out** 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。

distribute-list *acl* **out** [**interface** *if_name* | **eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

no distribute-list *acl* **out** [**interface** *if_name* | **eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

構文の説明

acl	標準アクセス リスト名。
connected	（任意）接続されたルートのみフィルタリングします。
eigrp *as_number*	（任意）指定した自律システム番号からの EIGRP ルートだけをフィルタリングします。*as_number* は、セキュリティ アプライアンス上の EIGRP ルーティング プロセスの自律システム番号です。
interface *if_name*	（任意）**nameif** コマンドで指定したインターフェイス名。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスに送信されたルーティング アップデートにのみ適用されます。
ospf *pid*	（任意）指定した OSPF プロセスにより検出された OSPF ルートのみフィルタリングします。
rip	（任意）RIP ルートのみフィルタリングします。
static	（任意）スタティック ルートのみフィルタリングします。

デフォルト

送信更新の場合、ネットワークはフィルタリングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	**eigrp** キーワードが追加されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての発信更新に適用されます。

例

次に、任意のインターフェイスから送信された RIP 更新で 10.0.0.0 ネットワークがアドバタイズされないようにする例を示します。

```
hostname(config)# access-list ripfilter deny 10.0.0.0
hostname(config)# access-list ripfilter permit any
```

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter out
```

次に、EIGRP ルーティング プロセスで外部インターフェイスの 10.0.0.0 ネットワークがアドバタイズされないようにする例を示します。

```
hostname(config)# access-list eigrp_filter deny 10.0.0.0
hostname(config)# access-list eigrp_filter permit any
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list eigrp_filter out interface outside
```

関連コマンド

コマンド	説明
distribute-list in	ルーティング アップデートで受信するネットワークをフィルタリングします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスのルータ 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。

dns domain-lookup

サポートされているコマンドに対してネーム ルックアップを実行するために、セキュリティ アプライアンスが DNS サーバに DNS 要求を送信すること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 **dns domain-lookup** コマンドを使用します。DNS ルックアップをディセーブルにするには、このコマンドの **no** 形式を使用します。

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

構文の説明

interface_name	DNS ルックアップをイネーブルにするインターフェイスを指定します。このコマンドを複数回入力して、DNS ルックアップを複数のインターフェイス上でイネーブルにする場合、セキュリティ アプライアンスは応答を受信するまで各インターフェイスを順番に試します。

デフォルト

デフォルトでは、DNS ルックアップ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
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

DNS 要求の送信先の DNS サーバ アドレスを設定するには、**dns name-server** コマンドを使用します。DNS ルックアップをサポートするコマンドのリストについては、**dns name-server** コマンドを参照してください。

セキュリティ アプライアンスは、ダイナミックに学習されたエントリで構成される名前解決のキャッシュを管理します。セキュリティ アプライアンスは、ホスト名から IP アドレスへの変換が必要になるたびに外部 DNS サーバにクエリーする代わりに、外部 DNS 要求から返された情報をキャッシュします。セキュリティ アプライアンスは、キャッシュにない名前に対してのみ要求を実行します。キャッシュのエントリは、DNS レコードの期限切れ、または 72 時間後のいずれか早い方に自動的にタイムアウトします。

例

次に、内部インターフェイス上で DNS ルックアップをイネーブルにする例を示します。

```
hostname(config)# dns domain-lookup inside
```

関連コマンド

コマンド	説明
dns name-server	DNS サーバ アドレスを設定します。
dns 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。
dns 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。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns-group（トンネル グループ webvpn コンフィギュレーション モード）

WebVPN トンネル グループに使用する DNS サーバを指定するには、トンネル グループ webvpn コンフィギュレーション モードで **dns-group** コマンドを使用します。デフォルトの DNS グループに戻すには、このコマンドの **no** 形式を使用します。

dns-group *name*

no dns-group

構文の説明

name	トンネル グループに使用する DNS サーバ グループ コンフィギュレーションの名前を指定します。

デフォルト

デフォルト値は DefaultDNS です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

名前には、任意の DNS グループを指定できます。dns-group コマンドはホスト名をトンネル グループの適切な DNS サーバに解決します。

dns server-group コマンドを使用して、DNS グループを設定します。

例

次に、「dnsgroup1」という名前の DNS グループの使用を指定するカスタマイゼーション コマンドの例を示します。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group dnsgroup1
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
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を 1 つまたはすべて表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

dns-guard

クエリーごとに 1 つの DNS 応答を実行する DNS Guard 機能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 **dns-guard** 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。

dns-guard

no dns-guard

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

DNS Guard 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で **no dns-guard** 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、動作は **global dns-guard** コマンドにより指定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

DNS ヘッダーの ID フィールドを使用して、DNS 応答と DNS ヘッダーを一致させます。クエリーごとに 1 つの応答がセキュリティ アプライアンスを介して許可されます。

例

次に、DNS インスペクション ポリシー マップで DNS Guard 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)# dns-guard
```

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。

dns 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 サーバのリストに再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** 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。

dns retries *number*

no dns retries [*number*]

構文の説明

number	再試行の回数を 0 ～ 10 の間で指定します。デフォルトは 2 です。

デフォルト

デフォルトの再試行回数は 2 回です。

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。
7.1(1)	このコマンドは、WebVPN 接続に対して廃止されました。

使用上のガイドライン

dns name-server コマンドを使用して DNS サーバを追加します。

例

次に、再試行回数を 0 回に設定する例を示します。セキュリティ アプライアンス により行われる試行は、各サーバに対して 1 回だけです。

```
hostname(config)# dns retries 0
hostname(config)#
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns 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。

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。
show dns-hosts	DNS キャッシュを表示します。

dns-server

プライマリおよびセカンダリの DNS サーバの IP アドレスを設定するには、グループ ポリシー コンフィギュレーション モードで **dns-server** 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。

dns-server {**value** *ip_address* [*ip_address*] | none}

no dns-server

構文の説明

none	dns サーバに、ヌル値を設定して DNS サーバを許可しません。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ DNS サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このオプションを使用すると、別のグループ ポリシーの DNS サーバを継承できます。サーバが継承されないようにするには、**dns-server none** コマンドを使用します。

dns-server コマンドを実行するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、次に DNS サーバ y.y.y.y を設定した場合、2 番めのコマンドは最初のコマンドを上書きし、y.y.y.y が唯一の DNS サーバになります。複数のサーバを設定する場合も同様です。以前に設定された DNS サーバを上書きする代わりにサーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを含めます。

例

次に、FirstGroup という名前のグループ ポリシーで、IP アドレスが 10.10.10.15、10.10.10.30、および 10.10.10.45 の DNS サーバを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

dns server-group

トンネル グループに使用する DNS サーバのドメイン名、ネーム サーバ、再試行回数、およびタイムアウトの値を指定できる DNS サーバ グループ モードを開始するには、グローバル コンフィギュレーション モードで **dns server-group** コマンドを使用します。特定の DNS サーバ 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。

dns server -group *name*

no dns server-group

構文の説明

name	トンネル グループに使用する DNS サーバ グループ コンフィギュレーションの名前を指定します。

デフォルト

デフォルト値は DefaultDNS です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

名前には、任意の DNS グループを指定できます。**dns server-group** コマンドを使用して、DNS グループを設定します。

例

次に、「eval」という名前の DNS サーバ グループを設定する例を示します。

```
hostname(config)# dns server-group eval
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 192.168.10.10
hostname(config-dns-server-group)# retries 5
hostname(config-dns-server-group)# timeout 7
hostname(config-dns-server-group)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

dns timeout

次の DNS サーバを試すまで待機する時間を指定するには、グローバル コンフィギュレーション モードで **dns timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

dns timeout *seconds*

no dns timeout [*seconds*]

構文の説明

seconds	タイムアウトを 1 ～ 30 の範囲で指定します（秒単位）。デフォルトは 2 秒です。セキュリティ アプライアンスがサーバのリストを再試行するたびに、このタイムアウトは倍増します。試行回数を設定するには、**dns retries** コマンドを参照してください。

デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、タイムアウトを 1 秒に設定します。

```
hostname(config)# dns timeout 1
```

関連コマンド

コマンド	説明
dns name-server	DNS サーバ アドレスを設定します。
dns 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。
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

domain-name

デフォルトのドメイン名を設定するには、グローバル コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、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、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバを修飾子を持たない名前の「jupiter」に指定した場合、セキュリティ アプライアンスによって名前は「jupiter.example.com」に修飾されます。

domain-name *name*

no domain-name [*name*]

構文の説明

name	ドメイン名を最大 63 文字で設定します。

デフォルト

デフォルト ドメイン名は default.domain.invalid です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マルチ コンテキスト モードでは、システム実行スペース内だけではなく、各コンテキストに対してドメイン名を設定できます。

例

次に、ドメインを example.com に設定する例を示します。

```
hostname(config)# domain-name example.com
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。

コマンド	説明
hostname	セキュリティ アプライアンスのホスト名を設定します。
show running-config domain-name	ドメイン名のコンフィギュレーションを表示します。

domain-name（dns サーバ グループ）

デフォルトのドメイン名を設定するには、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** コマンドを使用します。ドメイン名を削除するには、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、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバを修飾子を持たない名前の「jupiter」に指定した場合、セキュリティ アプライアンスによって名前は「jupiter.example.com」に修飾されます。

domain-name *name*

no domain-name [*name*]

構文の説明

name	ドメイン名を最大 63 文字で設定します。

デフォルト

デフォルト ドメイン名は default.domain.invalid 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
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)	**dns domain-lookup** コマンドはこのコマンドに置き換えられて廃止されました。

使用上のガイドライン

マルチ コンテキスト モードでは、システム実行スペース内だけではなく、各コンテキストに対してドメイン名を設定できます。

例

次に、ドメインを「dnsgroup1」の「example.com」に設定する例を示します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# domain-name example.com
hostname(config-dns-server-group)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。

コマンド	説明
domain-name	デフォルトのドメイン名をグローバルに設定します。
show running-config dns-server group	現在の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

downgrade

オペレーティング システム ソフトウェア（ソフトウェア イメージ）の以前のバージョンにダウングレードするには、特権 EXEC モードで **downgrade** コマンドを使用します。

注意　PIX セキュリティ アプライアンスが現在 PIX Version 7.0 以降を実行している場合は、以前のバージョンのソフトウェアをロードしないでください。PIX Version 7.0 ファイル システムがインストールされている PIX セキュリティ アプライアンスに、モニタ モードからソフトウェア イメージをロードすることは、予測できない動作を発生させるため、サポートされていません。ダウングレード プロセスを簡単に行うために用意された、実行中の PIX Version 7.0 イメージから、**downgrade** コマンドを使用することを強くお勧めします。

downgrade *image_url* **[activation-key [flash** | *4-part_key* | *file***]] [config** *start_config_url***]**

構文の説明

4-part_key	（任意）イメージに書き込むための 4 分割アクティベーション キーを指定します。 5 分割キーを使用する場合、4 分割キーに戻ることにより失われる可能性がある機能のリストと共に、警告が生成されます。 システム フラッシュが再フォーマットまたは消去された場合、ダウングレード用のデフォルト キーは使用できなくなります。その場合、CLI はコマンドラインにアクティベーション キーを入力するように求めます。これは、**activation-key** キーワードがコマンドラインで指定されていない場合のデフォルトの動作です。
activation-key	（任意）ダウングレードされたソフトウェア イメージで使用するアクティベーション キーを指定します。
config	（任意）スタートアップ コンフィギュレーション ファイルを指定します。
file	（任意）ダウングレード手順が完了した後で使用するパスまたは URL およびアクティベーション キー ファイルの名前を指定します。アップグレード プロセス中にフラッシュに保存されたファイルが、ソースのイメージ ファイルだった場合、このファイル内のアクティベーション キーがダウングレードで使用されます。
flash	（任意）5 分割アクティベーション キーを使用する前にデバイスで使用されていた 4 分割アクティベーション キーをフラッシュ メモリで検索するように指定します。これは、**activation-key** キーワードがコマンドラインで指定されていない場合のデフォルトの動作です。
image_url	ダウングレードするソフトウェア イメージのパスまたは URL および名前を指定します。ソフトウェア イメージは 7.0 の前のバージョンである必要があります。
start_config_url	（任意）ダウングレード手順が完了した後で使用するパスまたは URL およびコンフィギュレーション ファイルの名前を指定します。

デフォルト

activation-key キーワードが指定されていない場合、セキュリティ アプライアンスは最後に使用された 4 分割アクティベーション キーを試します。セキュリティ アプライアンスがフラッシュで 4 分割アクティベーション キーを検出できなかった場合、コマンドは拒否され、エラー メッセージが表示されます。この場合、次回にコマンドラインで有効な 4 分割アクティベーション キーを指定する必要があります。デフォルトのアクティベーション キーまたはユーザ指定のアクティベーション キーが、現在

有効なアクティベーション キーと比較されます。選択されたアクティベーション キーを使用することで、機能を損失する可能性がある場合、ダウングレード後に、損失する可能性のある機能のリストと共に警告が表示されます。

スタートアップ コンフィギュレーション ファイルが指定されていない場合、セキュリティ アプライアンスはデフォルトで downgrade.cfg を使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

バージョン	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

このコマンドは、ソフトウェア バージョン 7.0 以降を実行している Cisco PIX Firewall シリーズのセキュリティ アプライアンスに限り使用できます。このコマンドは、Cisco ASA 5500 シリーズのセキュリティ アプライアンスではサポートされていません。

注意　ダウングレード プロセス中に電源障害が発生すると、フラッシュ メモリが破損する場合があります。予防策として、ダウングレード プロセスを開始する前に、フラッシュ メモリ上のすべてのデータを外部デバイスにバックアップしてください。

破損したフラッシュ メモリを回復するためには、コンソールへの直接アクセスが必要です。詳細については、**format** コマンドを参照してください。

例

次の例では、ソフトウェアをバージョン 6.3.3 にダウングレードします。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
32c261f3 062afe24 c94ef2ea 0e299a3f
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm]
Installing the correct file system for the image and saving the buffered data
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Flash downgrade succeeded








Rebooting....

Enter zero actkey:
```

次の例は、無効なアクティベーション キーを入力した場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
0 0 0 0
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
Error: activation key entered is invalid.

Enter the file option when there is no actkey in the source image (happens if the source
is in tftp server).
```

次の例は、ソース イメージのアクティベーション キーを指定したときに、それが存在しなかった場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key file
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
Activation key does not exist in the source image.
Please use the activation-key option to specify an activation key.
```

次の例は、最後のプロンプトでダウングレード手順を中止する方法を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm] ===<typed n here>
Downgrade process terminated.
```

ダウングレードするには、ソフトウェア バージョンが 7.0 未満であることが必要です。次の例は、ソフトウェアのダウングレードに失敗した試行を示しています。

```
hostname# downgrade tftp://17.13.2.25//scratch/views/test/target/sw/cdisk
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Error: Need to use an image with version less than 7-0-0-0.
```

次の例は、イメージを指定したときにアクティベーション キーを確認しなかった場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.4.4.1-rel
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image checksum has not been verified
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Warning: Activation key not verified.
Key 32c261f3 633fe24 c94ef2ea e299a3f might be incompatible with the image version
4-4-1-0.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

次の例は、4 分割アクティベーション キーに、現在の 5 分割アクティベーション キーのすべての機能が含まれていない場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
The following features available in current activation key in flash
are NOT available in 4 tuple activation key in flash:
VPN-3DES-AES
GTP/GPRS
5 Security Contexts
Failover is different:
current activation key in flash: UR(estricted)
4 tuple activation key in flash: R(estricted)
Some features might not work in the downgraded image if this key is used.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

関連コマンド

コマンド	説明
copy running-config startup-config	現在の実行コンフィギュレーションをフラッシュ メモリに保存します。

download-max-size

ダウンロードするオブジェクトの最大許容サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **download-max-size** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

download-max-size <*size*>

no download-max-size

構文の説明

size	ダウンロードするオブジェクトの最大許容サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

サイズを 0 に設定すると、実質的にオブジェクトのダウンロードは許可されません。

例

次に、ダウンロードするオブジェクトの最大サイズを 1500 バイトに設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# download-max-size 1500
```

関連コマンド

コマンド	説明
post-max-size	ポストするオブジェクトの最大サイズを指定します。
upload-max-size	アップロードするオブジェクトの最大サイズを指定します。

コマンド	説明
webvpn	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 モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	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。WebVPN のグローバル設定を設定できます。

drop

match コマンドまたは **class** コマンドと一致するパケットをすべてドロップするには、一致またはクラス コンフィギュレーション モードで drop コマンドを使用します。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

drop [**send-protocol-error**] [**log**]

no drop [**send-protocol-error**] [**log**]

構文の説明

send-protocol-error	プロトコル エラー メッセージを送信します。
log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop** コマンドを使用して、**match** コマンドまたはクラス マップと一致するパケットをドロップします。この drop アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは **match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop** コマンドを入力して **match** コマンドまたは **class** コマンドと一致するすべてのパケットをドロップできます。

パケットをドロップすると、インスペクション ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションでパケットをドロップした場合は、それ以降、**match** コマンドまたは **class** コマンドと一致しません。最初のアクションがパケットのロギングである場合は、パケットのド

ロップなどの別のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットをドロップし、http-traffic クラス マップと一致した場合にログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

drop-connection

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop-connection** コマンドを使用してパケットをドロップし、**match** コマンドまたはクラス マップと一致するトラフィックの接続を閉じます。接続は、セキュリティ アプライアンス上の接続データベースから削除されます。接続がドロップされたセキュリティ アプライアンスに入る後続パケットはすべて廃棄されます。この drop-connection アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

drop-connection [**send-protocol-error**] [**log**]

no drop-connection [**send-protocol-error**] [**log**]

構文の説明

send-protocol-error	プロトコル エラー メッセージを送信します。
log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは **match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop-connection** コマンドを入力してパケットをドロップし、**match** コマンドまたは **class** コマンドと一致するトラフィックの接続を閉じます。

パケットをドロップするか、または接続を閉じると、インスペクション ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションがパケットをドロップし接続を閉じることである場合、それ以降は **match** コマンドまたは **class** コマンドに対応しません。最初のアクションがパケッ

トのロギングである場合は、パケットのドロップなどの別のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop-connection** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットをドロップし、接続を閉じて、http-traffic クラス マップと一致した場合にログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

dtls port

DTLS 接続用のポートを指定するには、webvpn コンフィギュレーション モードで **dtls port** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

dtls port *number*

no dtls port *number*

構文の説明

number	UDP ポート番号（1 ～ 65535）。

デフォルト

デフォルトのポート番号は 443 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、DTLS を使用する SSL VPN 接続用の UDP ポートを指定します。

DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

例

次に、webvpn コンフィギュレーション モードを開始し、DTLS 用にポート 444 を指定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# dtls port 444
```

関連コマンド

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

duplex

銅線イーサネット インターフェイス（RJ-45）のデュプレックス方式を設定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デュプレックス設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

duplex {**auto** | **full** | **half**}

no duplex

構文の説明

auto	デュプレックス モードを自動検出します。
full	デュプレックス モードを全二重に設定します。
half	デュプレックス モードを半二重に設定します。

デフォルト

デフォルトは auto です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

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

使用上のガイドライン

デュプレックス モードは、物理インターフェイス上にだけ設定します。

duplex コマンドは、ファイバ メディアでは使用できません。

ネットワークで自動検出がサポートされていない場合は、デュプレックス モードを特定の値に設定します。

ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

PoE ポート上でデュプレックス方式を **auto** 以外に設定した場合は、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコ ワイヤレス アクセス ポイントは検出されず、電源が供給されません。

例

次に、デュプレックス モードを全二重に設定する例を示します。

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

関連コマンド

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

dynamic-access-policy-config

DAP レコードとそれに関連付けられたアクセス ポリシー属性を設定するには、グローバル コンフィギュレーション モードで **dynamic-access-policy-config** コマンドを使用します。既存の DAP コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

DAP 選択コンフィギュレーション ファイルをアクティブにするには、activate 引数を指定して **dynamic-access-policy-config** コマンドを使用します。

dynamic-access-policy-config *name* | *activate*

no dynamic-access-policy-config

name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。
activate	DAP 選択コンフィギュレーション ファイルをアクティブにします。

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
name：グローバル コンフィギュレーション activeate：特権 EXEC	•	•	•	—	—

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

グローバル コンフィギュレーション モードで dynamic-access-policy-config コマンドを使用して、1 つまたは複数の DAP レコードを作成します。このコマンドを使用するには、ダイナミック アクセス ポリシー レコード モードを開始します。このモードでは、指定した DAP レコードの属性を設定できます。ダイナミック アクセス ポリシー レコード モードで使用できるコマンドは、次のとおりです。

- action
- description
- network-acl
- priority
- user-message
- webvpn

例

次に、user1 という名前の DAP レコードを設定する例を示します。

```
hostname(config)# dynamic-access-policy-config user1
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードにアクセス ポリシー属性を入力します。
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。

dynamic-access-policy-record

DAP レコードを作成してアクセス ポリシー属性を入力するには、グローバル コンフィギュレーション モードで **dynamic-access-policy-record** コマンドを使用します。既存の DAP レコ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。

dynamic-access-policy-record *name*

no dynamic-access-policy-record *name*

構文の説明

name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。

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
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

グローバル コンフィギュレーション モードで dynamic-access-policy-record コマンドを使用して、1 つまたは複数の DAP レコードを作成します。このコマンドを使用するには、ダイナミック アクセス ポリシー レコード モードを開始します。このモードでは、指定した DAP レコードの属性を設定できます。ダイナミック アクセス ポリシー レコード モードで使用できるコマンドは、次のとおりです。

- action
- description
- network-acl
- priority
- user-message
- webvpn

例

次に、Finance という名前の DAP レコードを作成する例を示します。

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

関連コマンド

コマンド	説明
clear config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定された DAP レコードを削除します。
dynamic-access-policy-config url	DAP 選択コンフィギュレーション ファイルを設定します。
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。