default コマンド～ duplex コマンド

default

time-range コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードのデフォルト設定を復元するには、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*}

シンタックスの説明

absolute	時間範囲が有効である絶対時間を定義します。
days-of-the-week	（オプション）最初の days-of-the-week 引数は、関連付けられている時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（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、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***to*** キーワードを入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、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*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 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。しかし、この機能は、NTP 同期化により最適に動作します。

例

次の例は、***absolute*** キーワードのデフォルト動作を復元する方法を示しています。

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

関連コマンド

コマンド	説明
absolute	時間範囲が有効であ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（crl 設定）

すべての CRL パラメータをシステムの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 モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバが必要とする場合にだけ使用されます。

default

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

このコマンドの呼び出しは、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

次の例では、ca-crl コンフィギュレーション モードに入り、CRL コマンド値をデフォルトに戻します。

```
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 モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol ldap	CRL の取得方法として LDAP を指定します。

default（時間範囲）

absolute コマンドおよび ***periodic*** コマンドのデフォルト設定を復元するには、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*}

シンタックスの説明

absolute	時間範囲が有効であ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時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（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、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***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

次の表は、このコマンドを入力できるモードを示しています。

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

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、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*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 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。しかし、この機能は、NTP 同期化により最適に動作します。

例

次の例は、***absolute*** キーワードのデフォルト動作を復元する方法を示しています。

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

関連コマンド

コマンド	説明
absolute	時間範囲が有効であ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 enrollment

すべての登録パラメータをシステムのデフォルト値に戻すには、暗号 CA トラストポイント コンフィギュレーション モードで **default enrollment** コマンドを使用します。

default enrollment

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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の一部になりません。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、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 モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。

default-domain

グループ ポリシーのユーザに対してデフォルトの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。

デフォルトのドメイン名をすべて削除するには、引数なしで **no default-domain** コマンドを使用します。**default-domain none** コマンドを発行して作成された null リストを含む設定済みのデフォルトのドメイン名がすべて削除されます。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 パケットにだけ適用されます。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。

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

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

シンタックスの説明

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 ポリシーからデフォルトのドメイン名を継承しないようにします。
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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトの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（.）だけです。

例

次の例は、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方法を示しています。

```
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、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

default-group-policy

デフォルトでユーザが継承するアトリビュートのセットを指定するには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **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*

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
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。トンネル グループ一般アトリビュート モードの **default-group-policy** コマンドで置き換えられています。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

デフォルトのグループ ポリシー DfltGrpPolicy では、セキュリティ アプライアンスが初期設定されています。すべてのトンネル グループ タイプにこのアトリビュートを適用できます。

例

次の例では、Config-general コンフィギュレーション モードに入り、「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アトリビュートのセットを指定します。このコマンドのセットは、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 グループを消去します。
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 グループの一般アトリビュートを指定します。

default-group-policy（webvpn）

WebVPN または電子メールのプロキシ コンフィギュレーションがグループ ポリシーを指定していない場合に、使用するグループ ポリシー名を指定するには、**default-group-policy** コマンドを使用します。WebVPN、IMAP4S、POP3S、および SMTPS セッションは、指定されたグループ ポリシーまたはデフォルトのグループ ポリシーのいずれかを必要とします。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メールの場合、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。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

default-group-policy *groupname*

no default-group-policy

シンタックスの説明

groupname	デフォルトのグループ 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。コンフィギュレーション モードで **group-policy** コマンドを使用し、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。**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のグループ ポリシーとして置き換えることができます。別の方法として、DfltGrpPolicy を編集することもできます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
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 グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート 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、削除できません。DefaultGroupPolicy の AVP は次のとおりです。

アトリビュート	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 minutes
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 アトリビュート：	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	mpme

例

次の例は、WebVPN に WebVPN7 という名前のデフォルト グループ ポリシーを指定する方法を示しています。

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

default-idle-timeout

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

デフォルトのアイドル タイムアウトを使用すると、セッションの失効を防ぐことができます。

default-idle-timeout *seconds*

no default-idle-timeout

シンタックスの説明

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、最大値は 1 日（86,400 秒）です。

デフォルト

1,800 秒（30 分）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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、または値が有効な範囲外である場合、セキュリティ アプライアンスはここで設定された値を使用します。

このコマンドに、短い時間を設定することをお勧めします。理由は、クッキーがディセーブルにされている（またはクッキーを要求され、それを拒否する）設定のブラウザにより、ユーザが接続していなくてもセッション データベースに表示される場合があるからです。許容する接続の最大数が 1 に設定されている場合は（**vpn-simultaneous-logins** コマンド）、すでに接続の最大数に達していることをデータベースが示すため、ユーザはログインし直すことができません。アイドル タイムアウトを低く設定すると、そのような実体のないセッションを迅速に削除し、ユーザは再度ログインできます。

例

次の例は、デフォルトのアイドル タイムアウトを 1,200 秒（20 分）に設定する方法を示しています。

```
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	許容する同時 VPN セッションの最大数を設定します。グループ ポリシーまたはユーザ名モードで使用します。

default-information originate（OSPF）

OSPF ルーティング ドメインへのデフォルトの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*]]

シンタックスの説明

always	（オプション）ソフトウェアでデフォルト ルートが設定されているかどうかかかわらず、常にデフォルト ルートをアドバタイズします。
metric *value*	（オプション）OSPF デフォルト メトリック値を指定します（0 ～ 16777214）。
metric-type {1 | 2}	（オプション）OSPF ルーティング ドメインにアドバタイズされたデフォルト ルートに関連する外部リンク タイプです。有効な値は次のとおりです。 • ***1***：タイプ 1 外部ルート • ***2***：タイプ 2 外部ルート
route-map *name*	（オプション）適用するルートマップの名前。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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共に使用すると、コマンドからオプションの情報だけが削除されます。たとえば、**no default-information originate** ***metric 3*** を入力すると、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。実行コンフィギュレーションからコマンド全体を削除するには、このコマンドの **no** 形式をオプションなしで使用します。つまり **no default-information originate** となります。

例

次の例は、オプションのメトリックおよびメトリック タイプと共に **default-information originate** コマンドを使用する方法を示しています。

```
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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

default-information originate（RIP）

RIP へのデフォルトの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*]

シンタックスの説明

route-map *name*	（オプション）適用するルートマップの名前。ルートマップが満たされると、ルーティング プロセスはデフォルトのルートを生成します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

次の例では、デフォルト ルートを RIP に生成する方法を示します。

```
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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

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*

シンタックスの説明

/noconfirm	（オプション）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	（オプション）指定されたファイルをすべてのサブディレクトリで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:	取り外しできない内蔵フラッシュを指定して、続けてコロン（:）を入力します。

デフォルト

ディレクトリを指定しない場合のデフォルトのディレクトリは、現在の作業ディレクトリです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

パスを指定しない場合、ファイルは現在の作業ディレクトリから削除されます。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。ファイルを削除する場合、ファイル名のプロンプトが表示され、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移動します。
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ているが、VPN 権限を持たないリモート ユーザに配信されるメッセージを変更するには、トンネル グループ webvpn コンフィギュレーション モードで **deny-message value** コマンドを使用します。

no deny-message value コマンドは、文字列を削除するので、リモート ユーザはメッセージを受信できません。

no deny-message none コマンドは、トンネル グループ ポリシー コンフィギュレーションからアトリビュートを削除します。ポリシーはアトリビュート値を継承します。

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

no deny-message value

no deny-message none

シンタックスの説明

string	最大 491 文字の英数字で、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。「ログインには成功しますが、特定の基準に適合しなかったり、一部の特定のグループ ポリシーがあったりする影響で、VPN 機能のいずれも使用する権限は与えられません。詳細については、IT 管理者にお問い合せください。」

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

このコマンドを入力する前に、グローバル コンフィギュレーション モードで **group-policy** *name* **attributes** を入力し、**webvpn** コマンドを入力します（すでに policy *name* を作成していることを前提としています）。

deny-message value コマンドで文字列を入力する場合は、コマンドが折り返しても続けて入力します。

VPN セッションで使用されるトンネル ポリシーとは別に、ログインの際にリモート ユーザのブラウザにこのテキストが表示されます。

例

次の例の最初のコマンドは group2 と呼ばれる内部グループ ポリシーを作成します。後続のコマンドは、そのポリシーに関連した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 コンフィギュレーション モードに入ります。
show running-config group-policy [*name*]	実行中のグループ ポリシー コンフィギュレーションを表示します（名前の付いたポリシーに対して）。
webvpn（グループ ポリシーまたはユーザ名コンフィギュレーション モード）	グループ ポリシー webvpn コンフィギュレーション モードに入ります。

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*

シンタックスの説明

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。許可される値は **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

次の表は、このコマンドを入力できるモードを示しています。

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

deny version コマンドを使用して、SNMP トラフィックを、SNMP の特定のバージョンに制限します。SNMP の以前のバージョンはセキュリティが低いため、セキュリティ ポリシーで SNMP トラフィックを Version 2 に制限することができます。**snmp-map** コマンドを使用して設定する SNMP マップ内で **deny version** コマンドを使用します。SNMP マップを作成した後で、**inspect snmp** コマンドを使用してマップをイネーブルにし、次に **service-policy** コマンドを使用して 1 つまたは複数のインターフェイスに適用します。

例

次の例は、SNMP トラフィックを識別し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# 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先のトラフィック クラスを定義します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
snmp-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 つまたは複数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、コンテキストまたはオブジェクト グループ）に対する説明を追加するには、さまざまな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。この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。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。

description *text*

no description

シンタックスの説明

text	説明に、最大 200 文字のテキスト文字列を設定します。文字列に疑問符（?）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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—
コンテキスト コンフィギュレーション	•	•	—	—	•
Gtp マップ コンフィギュレーション	•	•	•	•	—
インターフェイス コンフィギュレーション	•	•	•	•	•
オブジェクト グループ コンフィギュレーション	•	•	•	•	—
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、複数の新しいコンフィギュレーション モードに追加されました。

例

次の例は、「アドミニストレーション」コンテキスト コンフィギュレーションに説明を追加したものです。

```
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** コマンドで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 モードに入ります。
gtp-map	GTP 検査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 モードに入ります。
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** コマンドで指定され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 を通じてラーニングしたルートの管理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*

シンタックスの説明

distance	DHCP を通じてラーニングしたルートに適用する管理ディスタンス。有効な値は 1 ～ 255 です。

デフォルト

DHCP を通じてラーニングしたルートには、デフォルトで管理ディスタンス 1 が割り当てられます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

dhcp client route distance コマンドは、ルートが DHCP を通じてラーニングされる場合にのみチェックされます。DHCP を通じてルートをラーニングした後に **dhcp client route distance** コマンドを入力した場合、指定された管理ディスタンスはラーニング済みの既存のルートには影響しません。指定した管理ディスタンスが与えられるのは、このコマンドの入力後にラーニングされたルートだけです。

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

複数のインターフェイスで DHCP を設定した場合は、各インターフェイスについて **dhcp client route distance** コマンドを使用して、インストール済みルートの優先順位を指定する必要があります。

例

次の例では、GigabitEthernet0/2 上で DHCP を利用してデフォルト ルートを取得します。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 オペレーションによって、外部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監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で DHCP を通じて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、管理ディスタンス 254 が割り当てられています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
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 を通じてラーニングしたルートを、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	DHCP を通じて取得した IP アドレスを使用して、指定したインターフェイスを設定します。
sla monitor	SLA 監視オペレーションを定義します。
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 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

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

dhcp client route track コマンドは、DHCP を通じてルートをラーニングする場合にのみチェックされます。DHCP を通じてルートをラーニングした後に **dhcp client route track** コマンドを入力した場合、ラーニングした既存のルートは、トラッキング オブジェクトには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ラーニングされたルートだけです。

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

複数のインターフェイスで DHCP を設定した場合は、各インターフェイスについて **dhcp client route distance** コマンドを使用して、インストール済みルートの優先順位を指定する必要があります。

例

次の例では、GigabitEthernet0/2 上で DHCP を利用してデフォルト ルートを取得します。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 オペレーションによって、外部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監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で DHCP を通じて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、管理ディスタンス 254 が割り当てられています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
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 を通じてラーニングしたルートに管理ディスタンスを割り当てます。
ip address dhcp	DHCP を通じて取得した IP アドレスを使用して、指定したインターフェイスを設定します。
sla monitor	SLA 監視オペレーションを定義します。
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 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**}]

シンタックスの説明

both	クライアントは DHCP サーバが DNS A および PTR リソース レコードをアップデートするよう要求します。
none	クライアントは DHCP サーバが DDNS アップデートを実行しないよう要求します。
server	クライアントの要求を受信する DHCP サーバを指定します。

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 アップデートのみを実行するように要求します。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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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 モードで入力した場合、**dhcp client update dns** コマンドはグローバル コンフィギュレーション モードでこのコマンドで設定した設定値を上書きします。

例

次の例では、DHCP サーバが A RR と PTR RR のどちらもアップデートしないことをクライアントが要求するよう設定します。

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

次の例では、サーバが A RR と PTR RR をアップデートすることをクライアントが要求するよう設定します。

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

関連コマンド

コマンド	説明
ddns（**DDNS** アップデート方式モード）	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）	ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス 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 レコードを動的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。

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*

シンタックスの説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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、そのプールがイネーブルにされたセキュリティ 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、*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 Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例は、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 サーバを設定するため、**dhcpd address** コマンド、**dhcpd dns** コマンド、および **dhcpd enable** *interface_name* コマンドを使用する方法を示しています。

```
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
```

次の例は、内部インターフェイスに DHCP サーバを設定する方法を示しています。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	DHCP サーバの設定をすべて削除します。
dhcpd enable	指定したインターフェイス上で、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*]

シンタックスの説明

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 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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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に上書きされます。

例

次の例は、内部インターフェイス上で DHCP を設定する方法を示しています。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 autoconfig outside
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd enable	指定したインターフェイス上で、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消去するには、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*]

シンタックスの説明

dnsip1	DHCP クライアントに対するプライマリ DNS サーバの IP アドレスです。
dnsip2	（オプション）DHCP クライアントの代替 DNS サーバの IP アドレスです。
interface *if_name*	サーバに対して入力した値の適用対象とな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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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

次の例は、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 サーバを設定するため、**dhcpd address** コマンド、**dhcpd dns** コマンド、および **dhcpd enable** *interface_name* コマンドを使用する方法を示しています。

```
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	DHCP サーバの設定をすべて削除します。
dhcpd address	指定したインターフェイス上で 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上で、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 domain** コマンドを使用します。DNS ドメイン名を消去するには、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*]

シンタックスの説明

domain_name	example.com などの DNS ドメイン名。
interface *if_name*	サーバに対して入力した値の適用対象とな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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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

次の例は、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ために **dhcpd domain** コマンドを使用する方法を示しています。

```
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	DHCP サーバの設定をすべて削除します。
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、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。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は、セキュリティ アプライアンスが DHCP を使用して、接続されているクライアントを設定できることを意味します。

dhcpd enable *interface*

no dhcpd enable *interface*

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd enable *interface* コマンドを使用すると、DHCP デーモンが DHCP 対応のインターフェイス上で DHCP クライアントの要求のリッスンを開始します。**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、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 Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例は、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ために **dhcpd enable** コマンドを使用する方法を示しています。

```
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 サーバに対する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上で 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*]

シンタックスの説明

interface *if_name*	サーバに対して入力した値の適用対象とな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です。有効値は 300 ～ 1,048,575 秒です。

デフォルト

デフォルトの *lease_length* は 3,600 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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長を削除して、この値をデフォルト値の 3,600 秒に置き換えます。

例

次の例は、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ために **dhcpd lease** コマンドを使用する方法を示しています。

```
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	DHCP サーバの設定をすべて削除します。
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。オプションを消去するには、このコマンドの **no** 形式を使用します。**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。

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

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

シンタックスの説明

ascii	オプション パラメータが ASCII 文字列であることを指定します。
code	設定された DHCP オプションの番号を表します。有効値は 0 ～ 255 で、いくつかの例外があります。サポートしていない 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」の項を参照してください。
hex	オプション パラメータが 16 進文字列であることを指定します。
hex_string	16 進文字列を、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*	サーバに対して入力した値の適用対象とな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	10 進数の IP アドレスを指定します。
string	スペースなしの ASCII 文字列を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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、一般の発信規則が適用されます。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、一般の受信規則が適用されます。TFTP サーバ用のスタティック文と **access-list** 文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 に定義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、option 46 は 1 桁の 16 進値として RFC 2132 に定義されます。

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
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

例

次の例は、DHCP オプション 66 に TFTP サーバを指定する方法を示しています。

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

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
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*]

シンタックスの説明

interface *if_name*	サーバに対して入力した値の適用対象とな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 タイムアウト値です。最小値は 10、最大値は 10,000 です。デフォルトは 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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスは、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、1,500 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

次の例は、**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方法を示しています。

```
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	DHCP サーバの設定をすべて削除します。
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 アップデートを実行するには、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*]

シンタックスの説明

both	DHCP サーバが A と PTR の両方の DNS リソース レコード（RR）をアップデートするように指定します。
interface	DDNS アップデート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 アップデートのみを実行します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(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

ダイナミック DNS（DDNS）は、DNS で管理されている名前からアドレスへのマッピング、およびアドレスから名前へのマッピングをアップデートするものです。アップデートは 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アップデート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 タイプのリソース レコード（RR）に保持されます。

- A リソース レコードは、ドメイン名から IP アドレスへのマッピングを保持します。
- PTR リソース レコードは、IP アドレスからドメイン名へのマッピングを保持します。

DDNS アップデートを使用すると、A タイプの RR に保持される情報と、PTR タイプの RR に保持される情報との一貫性を維持できます。

dhcpd update dns コマンドを使用すると、DHCP サーバが A RR と PRT RR の両方アップデート、または PTR RR アップデート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アップデート要求を上書きするように設定することもできます。

例

次の例では、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 の両方のアップデートを実行するよう設定します。

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

関連コマンド

コマンド	説明
ddns（DDNS アップデート方式モード）	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）	ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス 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 レコードを動的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 クライアント用の 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。DHCP サーバから WINS サーバを削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

interface *if_name*	サーバに対して入力した値の適用対象とな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	（オプション）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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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

次の例は、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方法を示しています。

```
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	DHCP サーバの設定をすべて削除します。
dhcpd address	指定したインターフェイス上で 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 エージェントを使用すると、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*

シンタックスの説明

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名です。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcprelay enable *interface_name* コマンドによってセキュリティ アプライアンスが DHCP リレー エージェントを開始するようにするには、**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。そのコマンドがなければ、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 つのコンテキストの 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

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の 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上に設定し、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上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
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
```

次の例は、DHCP リレー エージェントをディセーブルにする方法を示しています。

```
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 エージェントに関する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	現在の DHCP リレー エージェント 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 リレー コンフィギュレーションから DHCP サーバを削除するには、このコマンドの **no** 形式を使用します。DHCP リレー エージェントを使用すると、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*]

シンタックスの説明

interface_name	DHCP サーバが常駐するセキュリティ アプライアンス インターフェイス名です。
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 アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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。**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、DHCP クライアントを設定することはできません。

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

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の 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上に設定し、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上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
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上で、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	現在の DHCP リレー エージェント 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*

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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 オプションがなければ、セキュリティ アプライアンスは、*interface* アドレスを含んでいるデフォルト 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

次の例は、**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方法を示しています。

```
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上で、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	現在の DHCP リレー エージェント 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

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の 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上に設定し、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上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
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上で、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	現在の DHCP リレー エージェント 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 モードで **dialog** コマンドを使用します。

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

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

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

シンタックスの説明

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

デフォルト

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

次の表は、このコマンドを入力できるモードを示しています。

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

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、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

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）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目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 を使用することをお勧めします。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のに便利な機能があります。

例

次の例では、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しています。

```
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]*

シンタックスの説明

/all	（オプション）すべてのファイルを表示します。
all-filesystems	（オプション）すべてのファイル システムのファイルを表示します。
/recursive	（オプション）ディレクトリの内容を再帰的に表示します。
system:	（オプション）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:	（オプション）デフォルト フラッシュ パーティションのディレクトリの内容を表示します。
path	（オプション）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のデフォルトのディレクトリは、現在の作業ディレクトリです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
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

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

次の例は、ディレクトリの内容を表示する方法を示しています。

```
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)
```

次の例は、ファイル システム全体の内容を再帰的に表示する方法を示しています。

```
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移動します。
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

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**enable** コマンドを使用して、特権モードに入ります。**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、特権モードに入る方法を示しています。

```
hostname> enable
hostname#
```

次の例は、特権モードを終了する方法を示しています。

```
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 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 アトリビュート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できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシングは頻繁に再利用されるオブジェクトをシステム キャッシュに保存します。キャッシュに保存しておくことにより、リライトやコンテンツの圧縮を繰り返し実行する必要が少なくなります。WebVPN とリモート サーバの間および WebVPN とエンドユーザのブラウザとの間の両方でトラフィックを削減します。その結果、多くのアプリケーションがさらに効率よく実行されます。

例

次の例は、キャッシングをディセーブルにする方法と、それを再度イネーブルにする方法を示しています。

```
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 モードに入ります。
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ングに関する再確認ポリシーを設定します。
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。

distance ospf

ルート タイプに基づいて OSPF ルートの管理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

シンタックスの説明

d1、*d2*、*d3*	各ルート タイプの距離です。有効な値は 1 ～ 255 です。
external	（オプション）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	（オプション）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	（オプション）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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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。管理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。管理ディスタンスを再入力する場合、対象ルート タイプの管理ディスタンスだけが変更されます。その他のルート タイプの管理ディスタンスは影響されません。

コマンドの **no** 形式には、キーワードも引数もありません。コマンドの **no** 形式を使用すると、すべてのルート タイプの管理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管理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

次の例では、外部ルートの管理ディスタンスを 150 に設定します。

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

次の例は、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方法を示しています。

```
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)#
```

次の例は、各管理ディスタンスを 105 に設定し、次に外部管理ディスタンスだけを 150 に変更する方法を示しています。**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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

distribute-list in

アップデートを受信した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** 形式を使用します。

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

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

シンタックスの説明

acl	標準アクセス リストの名前。
if_name	（オプション）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイスを指定すると、そのインターフェイス上で受信されたルーティング アップデートだけにアクセス リストが適用されます。

デフォルト

着信アップデートの場合、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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
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アップデートに適用されます。

例

次の例では、外部インターフェイスのルーティング アップデートのフィルタリングを制限します。10.0.0.0 ネットワークのルートを受け入れ、他はすべて拒否します。

```
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
```

関連コマンド

コマンド	説明
distribute-list out	RIP 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 rip	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

distribute-list out

RIP アップデートで特定のネットワークが送信されるの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** 形式を使用します。

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

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

シンタックスの説明

acl	標準アクセス リストの名前。
connected	（オプション）接続されたルートのみフィルタリングします。
interface *if_name*	（オプション）**nameif** コマンドで指定されたインターフェイスの名前。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 アップデートのみに適用されます。
ospf *pid*	（オプション）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	（オプション）RIP ルートのみフィルタリングします。
static	（オプション）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

送信アップデートの場合、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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
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ない場合、アクセス リストはすべての送信アップデートに適用されます。

例

次の例では、任意のインターフェイスから送信された RIP アップデートで 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
```

関連コマンド

コマンド	説明
distribute-list in	RIP アップデートで受信されるネットワークをフィルタリングします。
router rip	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内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 lookup 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*

シンタックスの説明

interface_name	DNS lookup 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 lookup 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 lookup はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
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 lookup 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、ダイナミックにラーニング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

次の例では、内部インターフェイス上で DNS lookup をイネーブルにします。

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

関連コマンド

コマンド	説明
dns name-server	DNS サーバの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、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
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 グループを復元するには、このコマンドの **no** 形式を使用します。

dns-group *name*

no dns-group

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(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

次の例は、「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 コマンドを示しています。

```
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 モードに入ります。
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 アトリビュートを設定する config-webvpn モードに入ります。

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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

DNS Guard はデフォルトでイネーブルです。このコマンドは、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定している場合は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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DNS ヘッダーのインデックス 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

次の例では、DNS 検査ポリシー マップで DNS Guard をイネーブルにする方法を示します。

```
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 マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

dns name-server

1 つまたは複数の DNS 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 **dns name-server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、WebVPN コンフィギュレーションまたは証明書コンフィギュレーションのサーバ名を解決するために DNS を使用します（サポートされるコマンドのリストについては、「使用上のガイドライン」を参照してください）。サーバ名を定義するその他の機能は（AAA など）、DNS 解決をサポートしていません。IP アドレスを入力するか、**name** コマンドを使用して手動により名前を IP アドレスに解決する必要があります。

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

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

シンタックスの説明

ip_address	DNS サーバの IP アドレスを指定します。最大 6 個のアドレスを個別のコマンドとして指定するか、利便性のために、1 つのコマンド内で 6 つまでのアドレスをスペースで分けて指定できます。1 つのコマンドに複数のサーバを入力する場合、セキュリティ アプライアンスは、各サーバをコンフィギュレーションの個別のコマンドに保存します。セキュリティ アプライアンスは、応答を受信するまで各 DNS サーバを順番に試します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは廃止されました。DNS サーバ グループ コンフィギュレーション モードの **name-server** コマンドで置き換えられています。

使用上のガイドライン

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

DNS 解決をサポートする WebVPN コマンドには、次のコマンドが含まれます。

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

DNS 解決をサポートする certificate コマンドには、次のコマンドが含まれます。

- **enrollment url**
- url

name コマンドを使用すると、名前と IP アドレスを手動で入力できます。

セキュリティ アプライアンスが一連の DNS サーバを再試行する回数を設定するには、**retries** コマンドを参照してください。

例

次の例では、3 つの DNS サーバを追加します。

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

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

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

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

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

それらを 2 つのコマンドとして入力することもできます。

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

複数のサーバを削除するには、それらのサーバを、次のように複数のコマンドとして、または 1 つのコマンドとして入力できます。

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

関連コマンド

コマンド	説明
domain-name（DNS サーバ グループ コンフィギュレーション モード）	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
name-server（DNS サーバ グループ コンフィギュレーション モード）	dns name-server コマンドの代わりに使用します。1 つ以上の DNS ネーム サーバを識別します。
retries（DNS サーバ グループ コンフィギュレーション モード）	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、一連の DNS サーバへのアクセスを再試行する回数を指定します。
timeout（DNS サーバ グループ コンフィギュレーション モード）	次の DNS サーバを試すまでに待つ時間を指定します。

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、一連の DNS サーバへのアクセスを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*]

シンタックスの説明

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

デフォルトでは、再試行の回数は 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
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

次の例では、再試行の回数を 0 に設定します。セキュリティ アプライアンスは各サーバを 1 回ずつ試します。

```
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 アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
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-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 モードで **dns-server** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、DNS サーバを別のグループ ポリシーから継承できます。サーバを継承しないようにするには、**dns-server none** コマンドを使用します。

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

no dns-server

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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 番目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。サーバを複数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

次の例は、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 サーバを設定する方法を示しています。

```
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、リトライ回数、タイムアウトの値を指定できる dns server-group モードに入るには、グローバル コンフィギュレーション モードで **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

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

次の例では、「eval」という名前の DNS サーバ グループを設定します。

```
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 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*]

シンタックスの説明

seconds	タイムアウトを 1 ～ 30 の間の秒単位で指定します。デフォルトは 2 秒です。セキュリティ アプライアンスが一連のサーバを試すたびに、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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、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 サーバの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、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
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拡張子として、ドメイン名を付加します。たとえば、ドメイン名を「example.com」と設定し、syslog サーバを、修飾子を持たない「jupiter」という名前で指定した場合、名前は、セキュリティ　　アプライアンスにより「jupiter.example.com.」と修飾されます。

domain-name *name*

no domain-name [*name*]

シンタックスの説明

name	ドメイン名を設定します。最大長は 63 文字です。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

マルチ コンテキスト モードの場合、システム実行スペース内だけでなく、各コンテキストでもドメイン名を設定できます。

例

次の例では、ドメインを example.com に設定します。

```
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 アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
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。

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 バージョン 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 バージョン 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 バージョン 7.0 イメージから、***downgrade*** コマンドを使用することをお勧めします。

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

シンタックスの説明

4-part_key	（オプション）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	（オプション）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	（オプション）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	（オプション）ダウングレード手順が完了した後で使用するパス /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	（オプション）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/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(1) 以前のバージョンである必要があります。
start_config_url	（オプション）ダウングレード手順が完了した後で使用するパス /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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
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、ソフトウェア リリース 7.0(1) 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、ソフトウェアをリリース 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 未満である必要があります。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。

drop

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 トラフィックの検査ポリシー 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 [**send-protocol-error**] [**log**]

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

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

検査ポリシー 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。検査ポリシー マップで使用できるコマンド自体は、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、検査ポリシー 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 2 番目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検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は検査ポリシー マップの名前です。

例

次の例では、パケットをドロップし、http-traffic クラス マップと一致した際にログを送信します。同じパケットが 2 番目の **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 マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

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後で、引き続きセキュリティ アプライアンスに入るパケットは廃棄されます。この drop-connection アクションはアプリケーション トラフィックの検査ポリシー 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**]

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

検査ポリシー 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。検査ポリシー マップで使用できるコマンド自体は、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したり接続を閉じると、それ以降は検査ポリシー マップでは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 2 番目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検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は検査ポリシー マップの名前です。

例

次の例では、http-traffic クラス マップと一致する際には、パケットをドロップし、接続を閉じてログを送信します。同じパケットが 2 番目の **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 マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

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

シンタックスの説明

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 検出です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

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

使用上のガイドライン

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。

ネットワークが自動検出をサポートしていない場合は、デュプレックス モードを特定の値に設定します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度またはデュプレックス方式のいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックス方式の両方に明示的に固定値を設定して、両方の設定に関するオートネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

PoE ポート上でデュプレックスを **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 およびシスコの無線アクセス ポイントは検出されず、電源が供給されません。

例

次の例では、デュプレックス モードを全二重に設定します。

```
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消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。