V

validate-attribute

RADIUSアカウンティングの使用時にRADIUS属性を検証するには、RADIUSアカウンティング パラメータ コンフィギュレーション モードで **validate-attribute** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。

validate-attribute [*attribute_number*]
no validate-attribute [*attribute_number*]

構文の説明

attribute_number	RADIUS アカウンティングで検証する RADIUS 属性。値の範囲は、1 ～ 191 です。ベンダー固有属性はサポートされません。

コマンド デフォルト

このオプションは、デフォルトで無効です。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを設定すると、セキュリティアプライアンスは、Framed IP属性に加えてRADIUS属性に対する照合も実行します。このコマンドは、インスタンスを複数設定できます。

RADIUS 属性のタイプのリストを見るには、次のサイトにアクセスしてください。

http://www.iana.org/assignments/radius-types

例

次に、ユーザー名 RADIUS 属性の RADIUS アカウンティングをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# validate-attribute 1
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクションポリシーマップのパラメータを設定します。

validate-kdc

アップロードされたキータブファイルを使用した Kerberos キー発行局（KDC）の認証を有効にするには、AAA サーバーグループモードで **validate-kdc** コマンドを使用します。KDC 認証を無効にするには、このコマンドの **no** 形式を使用します。

validate-kdc
no validate-kdc

コマンド デフォルト

このオプションは、デフォルトで無効です。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバーグループ	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(4)	このコマンドが追加されました。

使用上のガイドライン

validate-kdc コマンドを使用して、グループ内のサーバーを認証するように Kerberos AAA サーバーグループを設定できます。認証を実行するには、Kerberos キー発行局（KDC）からエクスポートしたキータブファイルもインポートする必要があります。KDC を検証することにより、攻撃者が KDC をスプーフィングして、ユーザークレデンシャルが攻撃者の Kerberos サーバーに対して認証されるようにする攻撃を防ぐことができます。

KDC の検証を有効にすると、チケット認可チケット（TGT）を取得してユーザーを検証した後、システムは **host**/*ASA_hostname* のユーザーに代わってサービスチケットも要求します。次にシステムは、返されたサービスチケットを KDC の秘密鍵に対して検証します。これは、KDC から生成され、ASA にアップロードされたキータブファイルに保存されます。KDC 認証に失敗すると、サーバーは信頼できないと見なされ、ユーザーは認証されません。

KDC 認証を完了するには、次の手順を実行する必要があります。

1. （KDC 上。）ASA の Microsoft Active Directory にユーザーアカウントを作成します（**Start > Programs > Administrative Tools > Active Directory Users and Computers** に移動します）。たとえば、ASA の完全修飾ドメイン名（FQDN）が asahost.example.com の場合は、asahost という名前のユーザーを作成します。

2. （KDC 上。）FQDN とユーザーアカウントを使用して、ASA のホストサービスプリンシパル名（SPN）を作成します。

```
C:> setspn -A HOST/asahost.example.com asahost
```

1. （KDC 上。）ASA の キータブファイルを作成します（わかりやすくするために改行を追加）。

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

1. （ASA 上。）**aaa kerberos import-keytab** コマンドを使用して、キータブ（この例では new.keytab）を ASA にインポートします。
2. （ASA 上。）Kerberos AAA サーバーグループ設定に **validate-kdc** コマンドを追加します。キータブファイルは、このコマンドが含まれているサーバーグループでのみ使用されます。

（注） Kerberos 制約付き委任（KCD）とともに KDC 検証を使用することはできません。サーバーグループが KCD に使用されている場合、**validate-kdc** コマンドは無視されます。

例

次に、FTP サーバー上に存在する new.keytab というキータブをインポートし、Kerberos AAA サーバーグループで KDC 検証を有効にする例を示します。

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab

ftp://ftpserver.example.com/new.keytab imported successfully
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos

ciscoasa(config-aaa-server-group)# validate-kdc
```

関連コマンド

コマンド	説明
aaa kerberos import-keytab	Kerberos キー発行局（KDC）からエクスポートされた Kerberos キータブファイルをインポートします。
clear aaa kerberos keytab	インポートされた Kerberos キータブファイルをクリアします。
show aaa kerberos keytab	Kerberos キータブファイルに関する情報を表示します。

validate-key

LISP メッセージの事前共有キーを指定するには、パラメータ コンフィギュレーション モードで**validate-key** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect lisp** コマンドを入力します。キーを削除するには、このコマンドの **no** 形式を使用します。

validate-key *key*
no validate-key *key*

構文の説明

key	LISP メッセージの事前共有キーを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

ASA が LISP メッセージの内容を読み取ることができるように、LISP 事前共有キーを指定します。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバーの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバーまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトの

みに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid,** および **validate-key** コマンドを参照してください。

2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフローモビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、EID を 10.10.10.0/24 ネットワーク上に制限して、事前共有キーを指定する例を示します。

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフローモビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。

コマンド	説明
site-id	クラスタ シャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

validation-policy

着信ユーザー接続に関連付けられている証明書を検証するためにトラストポイントを使用できる条件を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **validation-policy command** コマンドを使用します。指定した条件でトラストポイントを使用できないように指定するには、このコマンドの **no** 形式を使用します。

[**no**] **validation-policy** { **ssl-client | ipsec-client** } [**no-chain**] [**subordinate-only**]

構文の説明

ipsec-client	トラストポイントと関連付けられている認証局（CA）証明書およびポリシーを IPsec 接続の検証に使用できることを指定します。
no-chain	セキュリティデバイス上にない下位証明書のチェーンをディセーブルにします。
ssl-client	トラストポイントと関連付けられている認証局（CA）証明書およびポリシーを SSL 接続の検証に使用できることを指定します。
subordinate-only	このトラストポイントで表される CA から直接発行されたクライアント証明書の検証をディセーブルにします。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

リモート アクセス VPN では、導入要件に応じて、セキュア ソケット レイヤ（SSL）VPN、IP Security（IPsec）、またはこの両方を使用して、事実上すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。**validation-policy** コマンドを使用して、オンボード CA 証明書へのアクセスに使用できるプロトコルタイプを指定できます。

このコマンドで **no-chain** オプションを指定すると、ASA でトラストポイントとして設定されていない下位 CA 証明書が ASA でサポートされなくなります。

ASA では、同じ CA に対して 2 つのトラストポイントを保持できます。この場合は、同じ CA から 2 つの異なるアイデンティティ証明書が発行されます。トラストポイントが、この機能がイネーブルになっている別のトラストポイントにすでに関連付けられている CA に対して認証される場合、このオプションは自動的にディセーブルになります。これにより、パス検証パラメータの選択であいまいさが生じないようになります。ユーザーが、この機能をイネーブルにした別のトラストポイントにすでに関連付けられている CA に認証されたトラストポイントでこの機能を有効化しようとした場合、アクションは許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次に、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、このトラストポイントを SSL トラストポイントとして指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# validation-policy ssl
ciscoasa(config-ca-trustpoint)#
```

次に、トラストポイント checkin1 に対してクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントが指定したトラストポイントの下位証明書を受け入れるように設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# validation-policy subordinates-only
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
id-usage	トラストポイントの登録された ID の使用方法を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

validation-usage

このトラストポイントでの検証が許可される使用タイプを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **validation-usage command** を使用します。使用タイプを指定しない場合は、このコマンドの **no** 形式を使用します。

validation-usage ipsec-client | ssl-client | ssl-server
no validation-usage ipsec-client | ssl-client | ssl-server

構文の説明

ipsec-client	このトラストポイントを使用して IPsec クライアント接続を検証できることを示します。
ssl-client	このトラストポイントを使用して SSL クライアント接続を検証できることを示します。
ssl-server	このトラストポイントを使用して SSL サーバー証明書を検証できることを示します。

コマンド デフォルト

ipsec-client、ssl-client

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	client-types コマンドを置き換える目的でこのコマンドが追加されました。

使用上のガイドライン

同じ CA 証明書に関連付けられているトラストポイントが複数ある場合、特定のクライアント タイプに設定できるのは 1 つのトラストポイントだけです。ただし、1 つのトラストポイントを 1 つのクライアント タイプに設定し、別のトラストポイントを別のクライアント タイプに設定することができます。

同じ CA 証明書に関連付けられているトラストポイントがあり、これがすでに 1 つのクライアント タイプに設定されている場合は、この同じクライアント タイプ設定に新しいトラストポ

イントを設定することはできません。このコマンドの **no** 形式を使用して設定をクリアして、トラストポイントがいずれのクライアント検証にも使用できないようにすることができます。

リモート アクセス VPN では、導入要件に応じて、セキュア ソケット レイヤ（SSL）VPN、IP Security（IPsec）、またはこの両方を使用して、すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのクリプトCAトラストポイント コンフィギュレーション モードを開始します。

vdi

モバイルデバイスで実行される Citrix Receiver アプリケーションの XenDesktop および XenApp VDI サーバーへのセキュアなリモートアクセスを ASA 経由で提供するには、**vdi** コマンドを使用します。

vdi type citrix url *url* **domain** *domain* **username** *username* **password** *password*

構文の説明

domain ドメイン	仮想化インフラストラクチャ サーバーにログインするためのドメイン。この値は、クライアントレス マクロにすることができます。
password *password*	仮想化インフラストラクチャ サーバーにログインするためのパスワード。この値は、クライアントレス マクロにすることができます。
type	VDI のタイプ。Citrix Receiver タイプの場合、この値は *citrix* にする必要があります。
url *url*	http または https、ホスト名、ポート番号、および XML サービスへのパスを含む XenApp または XenDesktop サーバーの完全な URL。
username *username*	仮想化インフラストラクチャ サーバーにログインするためのユーザー名。この値は、クライアントレス マクロにすることができます。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

VDI モデルでは、管理者は、企業アプリケーションが事前にロードされているデスクトップをパブリッシュし、エンド ユーザーは、これらのデスクトップにリモート アクセスします。これらの仮想リソースは、ユーザーが Citrix Access Gateway を移動してアクセスする必要がないように、電子メールなどのその他のリソースと同様に表示されます。ユーザーは Citrix Receiver モバイル クライアントを使用して ASA にログオンし、ASA は事前定義された Citrix XenApp

または XenDesktop サーバーに接続されます。ユーザーが Citrix の仮想化されたリソースに接続する場合に、Citrix サーバーのアドレスおよびクレデンシャルをポイントするのではなく、ASA の SSL VPN IP アドレスおよびクレデンシャルを入力するように、管理者は [Group Policy] で Citrix サーバーのアドレスおよびログオン クレデンシャルを設定する必要があります。ASA がクレデンシャルを確認したら、受信側クライアントは ASA 経由で許可されているアプリケーションの取得を開始します。

サポートされているモバイル デバイス

- iPad：Citrix Receiver バージョン 4.x 以降
- iPhone/iTouch：Citrix Receiver バージョン 4.x 以降
- Android 2.x 電話機：Citrix Receiver バージョン 2.x 以降
- Android 3.x タブレット：Citrix Receiver バージョン 2.x 以降
- Android 4.0 電話機：Citrix Receiver バージョン 2.x 以降

例

ユーザー名とグループ ポリシーが両方とも設定されている場合、ユーザー名の設定は、グループ ポリシーに優先します。

```
configure terminal
 group-policy DfltGrpPolicy attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password   <password>
configure terminal
 username <username> attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password   <password>]
```

関連コマンド

コマンド	説明
debug webvpn citrix	Citrix ベースのアプリケーションおよびデスクトップを起動するプロセスの状況を知ることができます。

verify

ファイルのチェックサムを確認するには、特権 EXEC モードで **verify** コマンドを使用します。

verify*path*
verify { **/md5 | sha-512** } *path* [*expected_value*]
verify /signature running

構文の説明

/md5	指定したソフトウェア イメージの MD5 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
/sha-512	指定したソフトウェア イメージの SHA-512 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
/signature running	実行中の ASA イメージの署名を確認します。
expected_value	（オプション）指定したイメージの既知のハッシュ値。ハッシュ値が一致するか、または不一致があるかどうかを確認するメッセージが ASA に表示されます。

path	• **disk0:**/[*path*/]*filename* 内部フラッシュメモリを示します。**disk0** の代わりに **flash** を使用することもできます。これらはエイリアスになります。 • **disk1:**/[*path*/]*filename* 外部フラッシュメモリカードを示します。 • **flash:**/[*path*/]*filename* このオプションは、内部フラッシュカードを示します。**flash** は **disk0:** のエイリアスです。 • **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] 次のキーワードの 1 つを **type** として指定できます。 • **ap**：ASCII 受動モード • **an**：ASCII 通常モード • **ip**：（デフォルト）バイナリ受動モード • **in**：バイナリ通常モード • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] サーバーアドレスへのルートを上書きする場合は、インターフェイス名を指定します。 パス名にスペースを含めることはできません。パス名がスペースを含む場合は、**verify** コマンドではなく **tftp-server** コマンドでパスを設定します。 • **system:running-config** 実行コンフィギュレーションのハッシュを計算するか、または確認します。 • **system:text** ASA プロセスのテキストのハッシュを計算するか、または確認します。

コマンド デフォルト　現在のフラッシュ デバイスがデフォルトのファイル システムです。

（注）　**/md5** または **/sha-512** オプションを指定する場合、FTP、HTTP、TFTP などのネットワークファイルをソースとして使用できます。**/md5** または **/sha-512** オプションを指定せずに **verify** コマンドを使用した場合は、フラッシュのローカルイメージのみを確認できます。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.3(2)	**signature** キーワードが追加されました。
9.6(2)	**system:text** オプションが追加されました。

使用上のガイドライン

ファイルを使用する前にそのチェックサムを確認するには、**verify** コマンドを使用します。

ディスクで配布される各ソフトウェアイメージでは、イメージ全体に対して1つのチェックサムが使用されます。このチェックサムは、イメージをフラッシュ メモリにコピーする場合にのみ表示され、イメージファイルをあるディスクから別のディスクにコピーする場合は表示されません。

新しいイメージをロードまたは複製する前に、そのイメージのチェックサムと MD5 情報を記録しておき、イメージをフラッシュ メモリまたはサーバーにコピーするときにチェックサムを確認できるようにします。Cisco.com では、さまざまなイメージ情報を入手できます。

フラッシュメモリの内容を表示するには、**show flash** コマンドを使用します。フラッシュ メモリの内容のリストには、個々のファイルのチェックサムは含まれません。イメージをフラッシュメモリにコピーした後で、そのイメージのチェックサムを再計算して確認するには、**verify** コマンドを使用します。ただし、**verify** コマンドは、ファイルがファイルシステムに保存された後にのみ、整合性チェックを実行します。破損しているイメージが ASA に転送され、検出されずにファイルシステムに保存される場合があります。破損しているイメージが正常にASA に転送されると、ソフトウェアはイメージが壊れていることを把握できず、ファイルの確認が正常に完了します。

メッセージダイジェスト 5（MD5）ハッシュアルゴリズムを使用してファイルを検証するには、**/md5** オプションを指定して **verify** コマンドを使用します。MD5（RFC 1321 で規定）は、一意の 128 ビットのメッセージダイジェストを作成することによってデータの整合性を確認するアルゴリズムです。**verify** コマンドの **/md5** オプションを使用すると、ASA ソフトウェアイメージのMD5チェックサム値を、その既知のMD5チェックサム値と比較することによって、イメージの整合性を確認できます。すべてのセキュリティ アプライアンスのソフトウェア イメージの MD5 値は、ローカル システムのイメージの値と比較するために、Cisco.com から入手できるようになっています。SHA-512（**/sha-512**）も指定できます。

MD5 または SHA-512 整合性チェックを実行するには、**/md5** または **/sha-512** キーワードを指定して **verify** コマンドを発行します。たとえば、**verify /md5 flash:cdisk.bin** コマンドを発行すると、ソフトウェアイメージの MD5 値が計算されて表示されます。この値を、Cisco.com で入手できるこのイメージの値と比較します。

または、まず Cisco.com から MD5 値を取得し、その値をコマンド構文で指定できます。たとえば、**verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** コマンドを発行すると、MD5 値が一致するかどうかを示すメッセージが表示されます。MD5 値が一致しない場合は、いずれかのイメージが破損しているか、または入力した MD5 値が正しくありません。

例

次に、cdisk.bin というイメージファイルに対して使用された **verify** コマンドの例を示します。わかりやすくするために、一部のテキストは省略されています。

```
ciscoasa# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
ciscoasa#
```

次に、disk0 の署名イメージに対して使用された **verify** コマンドの例を示します。

```
ciscoasa(config)# verify lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Digital signature successfully validate
ciscoasa(config)# verify /signature lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Digital signature successfully validated
ciscoasa(config)# verify /signature cdisk.smp
Verifying file integrity of disk0:/cdisk.smp
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc6cc420aadfff8db42fae6088bc74959fdbc11f
Computed Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc6cc420aadfff8db42fae6088bc74959fdbc11f
CCO Hash      SHA-512:
cd5d459b6d2616e3530d9ed7c488b5a1b51269f19ad853fbf9c630997e716ded4fda61fa2afe6e293dc82f05997fd787b0ec22839c92a87a37811726e152fade
Signature Verified
ciscoasa(config)#
ciscoasa(config)# verify /signature corrupt.SSA
```

```
%ERROR: Signature algorithm not supported for file disk0:/corrupt.SSA.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
copy	ファイルをコピーします。
dir	システム内のファイルを一覧表示します。

verify-header

既知の IPv6 拡張ヘッダーだけを許可し、IPv6 拡張ヘッダーの順序を適用するには、パラメータ コンフィギュレーション モードで **verify-header** コマンドを適用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect ipv6** コマンドを入力します。これらのパラメータを無効にするには、このコマンドの **no** 形式を使用します。

verify-header { **order | type** }
no verify-header { **order | type** }

構文の説明

order	RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用します。
type	既知の IPv6 拡張ヘッダーのみを許可します。

コマンド デフォルト

順序とタイプの両方がデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

これらのパラメータは、デフォルトでイネーブルになっています。ディセーブルにするには、no キーワードを入力します。

例

次の例では、IPv6 インスペクション ポリシー マップの order および type パラメータをディセーブルにします。

```
ciscoasa(config)# policy-map type inspect ipv6 ipv6-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# no verify-header order
ciscoasa(config-pmap-p)# no verify-header type
```

関連コマンド

コマンド	説明
inspect ipv6	IPv6 インスペクションをイネーブルにします。
parameters	インスペクション ポリシーマップのパラメータ コンフィギュレーション モードを開始します。
policy-map type inspect ipv6	IPv6 インスペクション ポリシー マップを作成します。

version

ASA でグローバルに使用する RIP のバージョンを指定するには、ルータ コンフィギュレーション モードで **version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

version { **1 | 2** }
no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

コマンド デフォルト

ASA は、バージョン 1 およびバージョン 2 のパケットを受信しますが、送信するのはバージョン 1 のパケットのみです。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドと **rip receive version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、すべてのインターフェイスで RIP バージョン 2 のパケットを送受信するように ASA を設定する例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、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。

virtual http

仮想 HTTP サーバーを設定するには、グローバル コンフィギュレーション モードで **virtual http** コマンドを使用します。仮想サーバー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。

virtual http *ip_address*［ **warning** ］
no virtual http *ip_address*［ **warning** ］

構文の説明

ip_address	ASA 上の仮想 HTTP サーバーの IP アドレスを設定します。このアドレスは必ず、ASA にルーティングされる未使用のアドレスにしてください。
warning	（オプション）HTTP 接続を ASA にリダイレクトする必要があることをユーザーに通知します。このキーワードは、リダイレクトが自動的に行われないテキストベースのブラウザにのみ適用されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	以前のリリースで使用されていたインライン基本 HTTP 認証方式がリダイレクション方式に置き換えられたため、このコマンドは廃止され、不要になりました。
7.2(2)	**aaa authentication listener** コマンドを使用して、基本 HTTP 認証（デフォルト）と HTTP リダイレクションのいずれを使用するかを選択できるようになったため、このコマンドは復活しました。リダイレクション方式では、HTTP 認証をカスケードするための特別なコマンドは必要ありません。

使用上のガイドライン

ASA で HTTP 認証を使用する場合（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、ASA では、基本 HTTP 認証がデフォルトで使用されます。**redirect** キーワードを指定した **aaa authentication listener** を使用して、ASA によって、ASA 自体が生成した Web ページに HTTP 接続がリダイレクトされるように認証方式を変更できます。

ただし、基本 HTTP 認証の使用を続行する場合は、HTTP 認証をカスケードするときに **virtual http** コマンドが必要になることがあります。

ASA に加えて宛先 HTTP サーバーで認証が必要な場合は、 **virtual http** コマンドを使用して、ASA（AAA サーバー経由）と HTTP サーバーで別々に認証を受けることができます。仮想 HTTP を使用しない場合は、ASA に対する認証で使用したものと同じユーザー名とパスワードが HTTP サーバーに送信されます。HTTP サーバーのユーザー名とパスワードを別に入力するように求められることはありません。AAA サーバーと HTTP サーバーでユーザー名とパスワードが異なる場合、HTTP 認証は失敗します。

このコマンドは、AAA 認証を必要とするすべての HTTP 接続を ASA 上の仮想 HTTP サーバーにリダイレクトします。ASA により、AAA サーバーのユーザー名とパスワードの入力を求めるプロンプトが表示されます。AAA サーバーがユーザーを認証すると、ASA は HTTP 接続を元のサーバーにリダイレクトして戻しますが、AAA サーバーのユーザー名とパスワードは含めません。HTTP パケットにユーザー名とパスワードが含まれていないため、HTTP サーバーによりユーザーに HTTP サーバーのユーザー名とパスワードの入力を求めるプロンプトが別途表示されます。

着信ユーザー（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス リストに宛先インターフェイスとして仮想 HTTP アドレスも含める必要があります。さらに、NAT が必要ない場合でも（ **no nat-control** コマンドを使用）、仮想 HTTP IP アドレスに対する **static** コマンドを追加する必要があります。通常、アイデンティティ NAT コマンドが使用されます（アドレスを同一アドレスに変換）。

発信ユーザーについては、トラフィックの許可は明示的に行われますが、内部インターフェイスにアクセス リストを適用する場合は、必ず仮想 HTTP アドレスへのアクセスを許可してください。**static** ステートメントは不要です。

（注） **virtual http** コマンドを使用する場合は、**timeout uauth** コマンドの期間を 0 秒に設定しないでください。設定すると、実際の Web サーバーへの HTTP 接続ができなくなります。

例

次に、AAA 認証とともに仮想 HTTP をイネーブルにする例を示します。

```
ciscoasa(config)# virtual http 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq
http
ciscoasa(config)# access-list ACL-IN remark This is the HTTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
http
ciscoasa(config)# access-list ACL-IN remark This is the virtual HTTP address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list AUTH remark This is the HTTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list AUTH remark This is the virtual HTTP address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

関連コマンド

コマンド	説明
aaa authentication listener http	ASA が認証に使用する方式を設定します。
clear configure virtual	すべての **virtual** コマンドステートメントをコンフィギュレーションから削除します。
show running-config virtual	ASA 仮想サーバーの IP アドレスを表示します。
sysopt uauth allow-http-cache	**virtual http** コマンドをイネーブルにする場合は、このコマンドを使用すると、ブラウザキャッシュ内のユーザー名とパスワードを使用して仮想サーバーに再接続できます。
virtual telnet	ASA 上に仮想 Telnet サーバーを設定して、認証を必要とする他のタイプの接続を開始する前に、ユーザーを ASA で認証できるようにします。

virtual telnet

ASA 上に仮想 Telnet サーバーを設定するには、グローバル コンフィギュレーション モードで **virtual telnet** コマンドを使用します。ASA によって認証プロンプトが表示されない他のタイプのトラフィックに対する認証が必要な場合は、仮想 Telnet サーバーでユーザーを認証する必要があります。このサーバーを無効にするには、このコマンドの **no** 形式を使用します。

virtual telnet *ip_address*
no virtual telnet *ip_address*

構文の説明

ip_address	ASA 上の仮想 Telnet サーバーの IP アドレスを設定します。このアドレスは必ず、ASA にルーティングされる未使用のアドレスにしてください。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

任意のプロトコルまたはサービスのネットワークアクセス認証を設定できますが（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、HTTP、Telnet、または FTP のみで直接認証することもできます。ユーザーがまずこれらのサービスのいずれかで認証を受けておかないと、他のサービスは通過を許可されません。HTTP、Telnet、またはFTPのASAの通過を許可しない一方で、他のタイプのトラフィックを認証する場合は、ASA 上で設定された所定の IP アドレスにユーザーが Telnet で接続し、ASA によって Telnet プロンプトが表示されるように、仮想 Telnet を設定できます。

authentication match コマンドまたは **aaa authentication include** コマンドを使用して、仮想 Telnet アドレスへの Telnet アクセスに対しても、認証が必要なその他のサービスと同様、認証を設定する必要があります

認証が済んでいないユーザーが仮想 Telnet IP アドレスに接続すると、ユーザーはユーザー名とパスワードを求められ、その後 AAA サーバーにより認証されます。認証されると、ユーザーに [Authentication Successful.] というメッセージが表示されます。これで、ユーザーは認証が必要な他のサービスにアクセスできます。

着信ユーザー（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス リストに宛先インターフェイスとして仮想 Telnet アドレスも含める必要があります。さらに、NAT が必要ない場合でも（**no nat-control** コマンドを使用）、仮想 Telnet IP アドレスに対する **static** コマンドを追加する必要があります。通常、アイデンティティ NAT コマンドが使用されます（アドレスを同一アドレスに変換）。

発信ユーザーについては、トラフィックの許可は明示的に行われますが、内部インターフェイスにアクセス リストを適用する場合は、必ず仮想 Telnet アドレスへのアクセスを許可してください。**static** ステートメントは不要です。

ASA からログアウトするには、仮想 Telnet IP アドレスに再接続します。ログアウトするように求められます。

例

次に、他のサービスに対する AAA 認証とともに仮想 Telnet をイネーブルにする例を示します。

```
ciscoasa(config)# virtual telnet 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq
smtp
ciscoasa(config)# access-list ACL-IN remark This is the SMTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
telnet
ciscoasa(config)# access-list ACL-IN remark This is the virtual Telnet address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list AUTH remark This is the SMTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
ciscoasa(config)# access-list AUTH remark This is the virtual Telnet address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

関連コマンド

コマンド	説明
clear configure virtual	すべての **virtual** コマンドステートメントをコンフィギュレーションから削除します。
show running-config virtual	ASA 仮想サーバーの IP アドレスを表示します。
virtual http	ASA 上で HTTP 認証を使用しているときに、HTTP サーバーも認証を要求する場合は、このコマンドを使用して、ASA と HTTP サーバーで別々に認証を受けることができます。仮想 HTTP を使用しない場合は、ASA に対する認証で使用したものと同じユーザー名とパスワードが HTTP サーバーに送信されます。HTTP サーバーのユーザー名とパスワードを別に入力するように求められることはありません。

vlan（グループ ポリシー）

VLAN をグループポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで**vlan**コマンドを使用します。グループポリシーのコンフィギュレーションからVLAN を削除し、デフォルトのグループポリシーの VLAN 設定に置き換えるには、このコマンドの **no** 形式を使用します。

[**no**] **vlan** { *vlan_id* | **none** }

構文の説明

none	このグループ ポリシーに一致するリモート アクセス VPN セッションへの VLAN の割り当てをディセーブルにします。グループ ポリシーは、デフォルトのグループ ポリシーから vlan 値を継承しません。
vlan_id	このグループ ポリシーを使用するリモート アクセス VPN セッションに割り当てる VLAN の番号（10 進表記）。インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用して、この ASA に VLAN を設定する必要があります。

コマンド デフォルト

デフォルト値は none 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、このグループ ポリシーに割り当てられているセッションの出力 VLAN インターフェイスを指定します。ASA は、このグループのすべてのトラフィックを指定された VLAN に転送します。VLAN を各グループ ポリシーに割り当ててアクセス コントロールを簡素化できます。VLAN インターフェイス コンフィギュレーションを適用すると、クライアント間の通信が中断されます。2番目のクライアント宛てのパケットを含むすべてのパケットは、強制的にVLANインターフェイスに送信されます。クライアント間の通信を維持するために、パケットをファイアウォールに戻すには、デバイスのダウンストリームが必要です。

VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、VLAN マッピング オプションでは使用しないでください。vlan-mapping 設定によってパケットが間違ってルーティングされる可能性があるため、これらのインスペクション エンジンは、vlan-mapping 設定を無視します。

例

次のコマンドでは、VLAN 1 をグループ ポリシーに割り当てます。

```
ciscoasa(config-group-policy)# vlan 1
ciscoasa(config-group-policy)
```

次のコマンドでは、VLAN マッピングをグループ ポリシーから削除します。

```
ciscoasa(config-group-policy)# vlan none
ciscoasa(config-group-policy)
```

関連コマンド

コマンド	説明
show vlan	ASA に設定されている VLAN を表示します。
vlan（インターフェイス コンフィギュレーション モード）	サブインターフェイスに VLAN ID を割り当てます。
show vpn-session_summary.db	IPsec、Cisco AnyConnect、NAC の各セッションの数および使用中の VLAN の数を表示します。
show vpn-sessiondb	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。

vlan（インターフェイス）

VLAN IDをサブインターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。サブインターフェイスでは、トラフィックを通過させるために VLAN ID が必要です。VLAN サブインターフェイスを使用して、1 つの物理インターフェイスに複数の論理インターフェイスを設定できます。VLANを使用すると、所定の物理インターフェイス上で複数のセキュリティ コンテキストなどのトラフィックを別々に保管できます。

vlan *ID* [**secondary** *vlan_range*]
no vlan [**secondary** *vlan_range*]

構文の説明

id	1 ～ 4094 の範囲の整数を指定します。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。
secondary *vlan_range*	（オプション）1 つまたは複数のセカンダリ VLAN を指定します。*vlan_id* は、1 ～ 4094 の整数です。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。 セカンダリ VLAN は、（連続する範囲について）スペース、カンマ、およびダッシュで区切ることができます。ASA はセカンダリ VLAN でトラフィックを受信すると、そのトラフィックをプライマリ VLAN にマップします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**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。

リリース	変更内容
9.5(2)	**secondary** キーワードが追加されました。

使用上のガイドライン

1 つのプライマリ VLAN と 1 つまたは複数のセカンダリ VLAN を設定できます。ASA はセカンダリ VLAN でトラフィックを受信すると、それをプライマリ VLAN にマップします。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、ASA によって古い ID が変更されます。リストからいくつかのセカンダリ VLAN を削除するには、**no** コマンドを使用して削除する VLAN のみをリストすることができます。リストされた VLAN のみを選択的に削除できます。たとえば、範囲内の 1 つの VLAN を削除することはできません。

サブインターフェイスをイネーブルにするには、**no shutdown** コマンドを使用して物理インターフェイスをイネーブルにする必要があります。サブインターフェイスをイネーブルにする場合、通常は、物理インターフェイスをトラフィックが通過しないようにします。これは、物理インターフェイスはタグなしパケットを通過させるためです。したがって、インターフェイスを停止することによって物理インターフェイスを介したトラフィックの通過を防止することはできません。代わりに、**nameif** コマンドを省略することによって、トラフィックが物理インターフェイスを通過しないようにします。物理インターフェイスでタグなしパケットを通過させる場合は、通常どおり **nameif** コマンドを設定できます。

サブインターフェイスの最大数は、プラットフォームによって異なります。プラットフォームごとのサブインターフェイスの最大数については、CLI コンフィギュレーション ガイドを参照してください。

例

次に、VLAN 101 をサブインターフェイスに割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

次に、VLAN を 102 に変更する例を示します。

```
ciscoasa(config)# show running-config interface
gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-interface)# vlan 102
ciscoasa(config)# show running-config interface
gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
```

```
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

次に、一連のセカンダリ VLAN を VLAN 200 にマップする例を示します。

```
interface gigabitethernet 0/6.200
vlan 200 secondary 500 503 600-700
```

次に、リストからセカンダリ VLAN 503 を削除する例を示します。

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
vlan 200 secondary 500 600-700
no nameif
no security-level
no ip address
```

次に、Catalyst 6500 でどのように VLAN マッピングが機能するのかを示します。ノードを PVLANS に接続する方法については、Catalyst 6500 の設定ガイドを参照してください。

ASA の設定

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 の設定

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
```

```
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
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 running-config interface	インターフェイスの現在のコンフィギュレーションを表示します。

vpdn group

VPDN グループを作成または編集し、PPPoE クライアントを設定するには、グローバル コンフィギュレーション モードで **vpdn group** コマンドを使用します。コンフィギュレーションからグループポリシーを削除するには、このコマンドの **no** 形式を使用します。

vpdn group *group_name* { **localname** *username* **| request dialout pppoe | ppp authentication** { **chap | mschap | pap** } }
no vpdn group *group_name* { **localname** *name* **| request dialout pppoe | ppp authentication** { **chap | mschap | pap** } }

（注） PPPoEは、ASAでフェールオーバーを設定している場合、またはマルチコンテキストモードやトランスペアレントモードではサポートされません。PPPoEがサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

構文の説明

localname *username*	ユーザー名を認証のために VPDN グループにリンクし、**vpdn username** コマンドで設定された名前と照合する必要があります。
ppp authentication{chap | mschap | pap}}	ポイントツーポイント プロトコル（PPP）認証プロトコルを指定します。Windows クライアントのダイヤルアップ ネットワーク設定を使用して、使用する認証プロトコル（PAP、CHAP、またはMS-CHAP）を指定できます。クライアントで指定した設定は、セキュリティ アプライアンスで使用する設定と一致している必要があります。パスワード認証プロトコル（PAP）を使用すると、PPP ピアは相互に認証できます。PAP は、ホスト名またはユーザー名をクリアテキストで渡します。チャレンジ ハンドシェイク認証プロトコル（CHAP）を使用すると、PPP ピアは、アクセス サーバーとの通信によって不正アクセスを防止できます。MS-CHAP は Microsoft 版の CHAP です。PIX Firewall では、MS-CHAP バージョン 1 のみサポートされます（バージョン 2.0 はサポートされません）。 ホストで認証プロトコルが指定されていない場合は、コンフィギュレーションで ppp authentication オプションを指定しないでください。
request dialout pppoe	ダイヤルアウト PPPoE 要求を許可することを指定します。
vpdn group *group_name*	VPDN グループの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

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

使用上のガイドライン

バーチャル プライベート ネットワーク（VPDN）は、リモート ダイヤルイン ユーザーとプライベート ネットワーク間の長距離のポイントツーポイント接続を提供するために使用します。セキュリティ アプライアンス上の VDPN では、レイヤ 2 トンネリング技術の PPPoE を使用して、リモート ユーザーからパブリック ネットワーク経由のプライベート ネットワークへのダイヤルアップ ネットワーク接続を確立します。

PPPoE は、Point-to-Point Protocol（PPP）over Ethernet です。PPP は、IP、IPX、ARA などのネットワーク層プロトコルで動作するように設計されています。PPP には、セキュリティ メカニズムとして CHAP と PAP も組み込まれています。

PPPoE 接続のセッション情報を表示するには、**show vpdn session pppoe** コマンドを使用します。コンフィギュレーションからすべての **vpdn group** コマンドを削除して、すべてのアクティブな L2TP トンネルと PPPoE トンネルを停止するには、**clear configure vpdn group** コマンドを使用します。**clear configure vpdn username** コマンドは、コンフィギュレーションからすべての **vpdn username** コマンドを削除します。

PPPoE は PPP をカプセル化するため、PPPoE は PPP を使用して、認証および VPN トンネル内で動作しているクライアント セッションに対する ECP 機能と CCP 機能を実行します。さらに、PPP によって PPPoE に IP アドレスが割り当てられるため、PPPoE と DHCP の併用はサポートされません。

（注） PPPoE に VPDN グループが設定されていない場合、PPPoE は接続を確立できません。

PPPoE に使用する VPDN グループを定義するには、**vpdn group** *group_name* **request dialout pppoe** コマンドを使用します。次に、インターフェイス コンフィギュレーション モードで **pppoe client vpdn group** コマンドを使用して、VPDN グループを特定のインターフェイス上の PPPoE クライアントに関連付けます。

ISP が認証を要求している場合は、**vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} コマンドを使用して、ISP で使用される認証プロトコルを選択します。

ISP によって割り当てられたユーザー名を VPDN グループに関連付けるには、**vpdn group** *group_name* **localname** *username* コマンドを使用します。

PPPoE 接続用のユーザー名とパスワードのペアを作成するには、**vpdn username** *username* password *password* コマンドを使用します。ユーザー名は、PPPoE に指定した VPDN グループにすでに関連付けられているユーザー名にする必要があります。

（注） ISP で CHAP または MS-CHAP が使用されている場合、ユーザー名はリモート システム名、パスワードは CHAP シークレットと呼ばれることがあります。

PPPoE クライアント機能はデフォルトでオフになっているため、VPDN の設定後、**ip address** *if_name* **pppoe** [**setroute**] コマンドを使用して PPPoE をイネーブルにします。setroute オプションを指定すると、デフォルト ルートが存在しない場合にデフォルト ルートが作成されます。

PPPoE の設定後すぐに、セキュリティ アプライアンスは通信する PPPoE アクセス コンセントレータを探します。PPPoE 接続が正常終了または異常終了すると、ASA は通信する新しいアクセス コンセントレータを探します。

次の **ip address** コマンドは、PPPoE セッションの開始後に使用しないでください。使用すると、PPPoE セッションが終了します。

- **ip address outside pppoe**：このコマンドは、新しい PPPoE セッションを開始しようとするためです。
- **ip address outside dhcp**：このコマンドは、インターフェイスがその DHCP 設定を取得するまでインターフェイスをディセーブルにするためです。
- **ip address outside** *address netmask*：このコマンドは、正常に初期化されたインターフェイスとしてインターフェイスを起動させるためです。

例

次に、VDPN グループ *telecommuters* を作成し、PPPoE クライアントを設定する例を示します。

```
ciscoasa(config)# vpdn group telecommuters request dialout pppoe
ciscoasa(config)# vpdn group telecommuters localname user1
ciscoasa(config)# vpdn group telecommuters ppp authentication pap
ciscoasa(config)# vpdn username user1 password test1
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-subif)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての vpdn group コマンドをコンフィギュレーションから削除します。

コマンド	説明
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show vpdn group *group_name*	VPDN グループのコンフィギュレーションを表示します。
vpdn username	PPPoE接続用のユーザー名とパスワードのペアを作成します。

vpdn username

PPPoE接続用のユーザー名とパスワードのペアを作成するには、グローバル コンフィギュレーション モードで **vpdn username** コマンドを使用します。

vpdn username *username* **password** *password* ［ **store-local** ］
no vpdn username *username* **password** *password* ［ **store-local** ］

（注） PPPoEは、ASAでフェールオーバーを設定している場合、またはマルチコンテキストモードやトランスペアレントモードではサポートされません。PPPoEがサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

構文の説明

password	パスワードを指定します。
store-local	ユーザー名とパスワードをセキュリティ アプライアンス上の NVRAM の特別な場所に保存します。Auto Update Server が clear config コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティアプライアンスはNVRAMからユーザー名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。
username	ユーザー名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。「使用上のガイドライン」を参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

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

使用上のガイドライン

VPDN ユーザー名は、**vpdn group** *group_name* **localname** *username* コマンドで指定された VPDN グループにすでに関連付けられているユーザー名にする必要があります。

clear configure vpdn username コマンドは、コンフィギュレーションからすべての **vpdn username** コマンドを削除します。

例

次に、パスワードが *telecommuter*9/8 の *bob_smith* という VPDN ユーザー名を作成する例を示します。

```
ciscoasa(config)# vpdn username bob_smith password telecommuter9/8
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての **vpdn group** コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての **vpdn username** コマンドをコンフィギュレーションから削除します。
show vpdn group	VPDN グループのコンフィギュレーションを表示します。
vpdn group	VPDN グループを作成し、PPPoE クライアントを設定します。

vpn-access-hours

グループポリシーを設定済み time-range ポリシーに関連付けるには、グループ ポリシー コンフィギュレーションモードまたはユーザー名コンフィギュレーションモードで **vpn-access-hours** 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この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、他のグループ ポリシーから time-range 値を継承できます。値が継承されないようにするには、**vpn-access-hours none** コマンドを使用します。

vpn-access hours value { *time-range* } **| none**
no vpn-access hours

構文の説明

none	VPN アクセス時間をヌル値に設定して、time-range ポリシーを許可しないようにします。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。
time-range	設定済みの時間範囲ポリシーの名前を指定します。

コマンド デフォルト

制限なし。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、FirstGroup というグループ ポリシーを 824 という time-range ポリシーに関連付ける例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-access-hours 824
```

関連コマンド

コマンド	説明
time-range	ネットワークにアクセスする曜日と 1 日の時間を設定します（開始日と終了日を含む）。

vpn-addr-assign

IPv4 アドレスをリモート アクセス クライアントに割り当てる方法を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** 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。設定されている VPN アドレスの割り当て方法を ASA からすべて削除するには、引数なしで、このコマンドの **no** 形式を使用します。

vpn-addr-assign { **aaa | dhcp | local** [**reuse-delay** *delay*] }
no vpn-addr-assign { **aaa | dhcp | local** [**reuse-delay** *delay*] }

構文の説明

aaa	外部または内部（ローカル）AAA 認証サーバーから IPv4 アドレスを割り当てます。
dhcp	DHCP 経由で IP アドレスを取得します。
local	ASA に設定されている IP アドレスプールから IP アドレスを割り当てて、トンネルグループに関連付けます。
reuse-delay *delay*	解放された IP アドレスを再利用するまでの遅延時間。指定できる範囲は 0 ～ 480 分です。デフォルトは 0（ディセーブル）です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(3)	reuse-delay オプションが追加されました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

DHCP を選択する場合は、**dhcp-network-scope** コマンドを使用して、DHCP サーバーが使用できる IP アドレスの範囲も定義する必要があります。DHCP サーバーが使用する IP アドレスを指定するには、dhcp-server コマンドを使用する必要があります。

ローカルを選択する場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要もあります。次に、**vpn-framed-ip-address** コマンドと **vpn-framed-netmask** コマンドを使用して、IP アドレスとネットマスクを個々のユーザーに割り当てます。

ローカル プールを使用する場合は、reuse-delay delay オプションを使用して、解放された IP アドレスを再利用するまでの遅延時間を調整します。遅延時間を長くすると、IP アドレスがプールに戻されて即座に再割り当てされるときにファイアウォールで発生する可能性がある問題を回避できます。

AAA を選択する場合は、設定済みのいずれかの RADIUS サーバーから IP アドレスを取得します。

例

次に、アドレス割り当て方法として DHCP を設定する例を示します。

```
ciscoasa
(config)#
 vpn-addr-assign dhcp
```

関連コマンド

コマンド	説明
dhcp-network-scope	ASA DHCP サーバーがグループポリシーのユーザーにアドレスを割り当てるために使用する IP アドレスの範囲を指定します。
ip-local-pool	ローカル IP アドレス プールを作成します。
ipv6-addr-assign	リモート アクセス クライアントに IPv6 アドレスを割り当てる方法を指定します。
vpn-framed-ip-address	特定のユーザーに割り当てる IP アドレスを指定します。
vpn-framed-ip-netmask	特定のユーザーに割り当てるネットマスクを指定します。

vpn-mode

クラスタにVPNモードを指定するには、クラスタ グループ コンフィギュレーション モードで **vpn-mode** コマンドを使用します。vpn-modeのクラスタリング コマンドを使用すると、管理者は集中型モードと分散型モードを切り替えることができます。VPN モード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。CLI のバックアップ オプションを使用すると、管理者は VPN セッションのバックアップを別のシャーシに作成するかどうかを設定できます。このコマンドの no 形式を使用すると、設定はデフォルト値に戻ります。

vpn-mode [**centralized | distributed**] [**backup** { **flat | remote-chassis** }]
[**no**] **vpn-mode** [**centralized | distributed** { **flat | remote-chassis** }]

コマンド デフォルト

デフォルトの VPN モードは集中型です。デフォルトのバックアップはフラットです。

構文の説明

centralized	VPN セッションは集中管理され、クラスタ マスター ユニットでのみ実行されます。
distributed	VPN セッションは、クラスタのメンバーに分散されます。
flat	バックアップ セッションは、クラスタの他のメンバーに割り当てられます。
remote-chassis	バックアップ セッションは、別のシャーシのメンバーに割り当てられます。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスタ構成	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.9(1)	このコマンドが追加されました。

使用上のガイドライン

フラット バックアップ モードでは、他のクラスタ メンバーにスタンバイ セッションが確立されます。これにより、ユーザーはブレード障害から保護されますが、シャーシ障害の保護は保証されません。

リモートシャーシ バックアップ モードでは、クラスタ内の別のシャーシのメンバーにスタンバイ セッションが確立されます。これにより、ユーザーはブレード障害とシャーシ障害の両方から保護されます。

リモートシャーシが単一のシャーシ環境（意図的に構成されたものまたは障害の結果）で構成されている場合、別のシャーシが結合されるまでバックアップは作成されません。

例

```
ciscoasa (cfg-cluster)# vpn-mode distributed
Return the backup strategy of a distributed VPN cluster to default:
no vpn-mode distributed backup
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループの設定を行います。
show cluster vpn-sessiondb distribution	クラスタ メンバー間のアクティブ セッションとバックアップ セッションの分布を表示します。

vpnclient connect

設定済みサーバーへのEasy VPN Remote接続の確立を試行するには、グローバル コンフィギュレーション モードで **vpnclient connect** コマンドを使用します。

vpnclient connect

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

例

次に、設定済み EasyVPN サーバーへの Easy VPN リモート接続の確立を試行する例を示します。

```
ciscoasa
(config)#
vpnclient connect
ciscoasa
(config)#
```

vpnclient enable

Easy VPN Remote 機能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 **vpnclient enable** コマンドを使用します。Easy VPN Remote 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。

vpnclient enable
no vpnclient enable

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

vpnclient enable コマンドを入力すると、サポートされる ASA は Easy VPN Remote ハードウェア クライアントとして機能します。

例

次に、Easy VPN Remote 機能をイネーブルにする例を示します。

```
ciscoasa
(config)#
vpnclient enable
ciscoasa
(config)#
```

次に、Easy VPN Remote 機能をディセーブルにする例を示します。

```
ciscoasa
(config)#
```

```
no
vpnclient enable
ciscoasa
(config)#
```

vpnclient ipsec-over-tcp

Easy VPN Remote ハードウェアクライアントとして動作している ASA を、TCP カプセル化 IPsec を使用するように設定するには、グローバル コンフィギュレーション モードで **vpnclient ipsec-over-tcp** 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この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。

vpnclient ipsec-over-tcp [**port** *tcp_port*]
no vpnclient ipsec-over-tcp

構文の説明

port	（任意）特定のポートを使用するように指定します。
tcp_port	（**port** キーワードを指定する場合は必須）TCP カプセル化 IPsec トンネルに使用する TCP ポート番号を指定します。

コマンド デフォルト

コマンドでポート番号を指定しない場合、Easy VPN Remote 接続では、ポート 10000 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

デフォルトでは、Easy VPN クライアントおよびサーバーは、IPsec を User Datagram Protocol（UDP）パケットにカプセル化します。一部の環境（特定のファイアウォール ルールが設定されている環境など）または NAT デバイスや PAT デバイスでは、UDP を使用できません。そのような環境で標準のカプセル化セキュリティ プロトコル（ESP、プロトコル 50）またはインターネット キー エクスチェンジ（IKE、UDP 500）を使用するには、TCP パケット内に IPsec をカプセル化してセキュアなトンネリングをイネーブルにするようにクライアントとサーバー

を設定します。ただし、UDP が許可されている環境では、IPsec over TCP を設定すると不要なオーバーヘッドが発生します。

TCP カプセル化 IPsec を使用するように ASA を設定する場合は、次のコマンドを入力して、外部インターフェイスを介して大きなパケットを送信できるようにします。

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

このコマンドは、Don't Fragment（DF）ビットをカプセル化されたヘッダーからクリアします。DF ビットは、パケットを断片化できるかどうかを決定する IP ヘッダー内のビットです。このコマンドを使用すると、Easy VPN ハードウェア クライアントは MTU サイズよりも大きいパケットを送信できます。

例

次に、デフォルト ポート 10000 を使用して TCP カプセル化 IPsec を使用するように Easy VPN Remote ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
ciscoasa
(config)#
vpnclient ipsec-over-tcp
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa
(config)#
```

次に、ポート 10501 を使用して TCP カプセル化 IPsec を使用するように Easy VPN Remote ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
ciscoasa
(config)#
vpnclient ipsec-over-tcp port 10501
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa
(config)#
```

vpnclient mac-exempt

Easy VPN Remote 接続の背後にあるデバイスに対して個々のユーザー認証要件を免除するには、グローバル コンフィギュレーション モードで **vpnclient mac-exempt** 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この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。

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]
no vpnclient mac-exempt

構文の説明

mac_addr_1	ドット付き 16 進表記の MAC アドレス。個々のユーザー認証を免除するデバイスの製造業者とシリアル番号を指定します。デバイスが複数の場合は、スペースで区切った各 MAC アドレスとそれぞれのネットワークマスクを指定します。 MAC アドレスの最初の 6 文字はデバイスの製造業者を識別し、最後の 6 文字はシリアル番号です。最後の 24 ビットは、ユニットの 16 進形式のシリアル番号です。
mac_mask_1	対応する MAC アドレスのネットワーク マスク。スペースを使用して、ネットワーク マスク、および後続の MAC アドレスとネットワーク マスクのペアを区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

Cisco IP Phone、無線アクセス ポイント、プリンタなどのデバイスは、認証を実行できないため、個々のユニット認証がイネーブルになっている場合でも認証されません。個々のユーザー認証がイネーブルになっている場合は、このコマンドを使用してこれらのデバイスの認証を免除できます。デバイスに対する個々のユーザー認証の免除は、「デバイス パススルー」とも呼ばれます。

このコマンドでは、MAC アドレスとマスクは、3 つの 16 進数をピリオドで区切って指定します。たとえば、MAC マスク ffff.ffff.ffff は、指定した MAC アドレスとのみ一致します。すべてがゼロのMACマスクは、いずれのMACアドレスとも一致しません。MACマスク ffff.ff00.0000 は、製造業者が同じであるすべてのデバイスと一致します。

（注） ヘッドエンド デバイス上で設定された個別ユーザー認証およびユーザー バイパスが必要です。たとえば、ヘッドエンドデバイスとしての ASA がある場合は、グループポリシーに従って次のように設定します。ciscoasa(config-group-policy)# **user-authentication enable**ciscoasa(config-group-policy)# **ip-phone-bypass enable**

例

Cisco IP Phone には、製造業者 ID として 00036b が設定されています。したがって、次のコマンドは、今後追加される可能性がある Cisco IP Phone も含めてすべての Cisco IP Phone を免除します。

```
ciscoasa
(config)#
vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
ciscoasa
(config)#
```

次に、1 つの特定の Cisco IP Phone を免除する例を示します。このようにすると、セキュリティは向上しますが、柔軟性が低くなります。

```
ciscoasa
(config)#
vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
ciscoasa
(config)#
```

vpnclient management

Easy VPN Remote ハードウェアクライアントへの管理アクセス用の IPsec トンネルを生成するには、グローバル コンフィギュレーション モードで **vpnclient management** コマンドを使用します。

vpnclient management tunnel *ip_addr_1 ip_mask_1* ［ *ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n* ］
vpnclient management clear

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。これにより、管理専用の IPsec トンネルが **split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って設定されます。

no vpnclient management clear

構文の説明

clear	通常のルーティングを使用して、社内ネットワークから Easy VPN クライアントとして動作している ASA 5505 の外部インターフェイスへの管理アクセスを提供します。このオプションでは、管理トンネルは作成されません。 （注） このオプションは、クライアントとインターネット間で NAT デバイスが動作している場合に使用します。
ip_addr	Easy VPN ハードウェア クライアントからの管理トンネルを構築するホストまたはネットワークの IP アドレス。この引数は、**tunnel** キーワードとともに使用します。スペースで区切った 1 つ以上の IP アドレスとそれぞれのネットワーク マスクを指定します。
ip_mask	対応する IP アドレスのネットワーク マスク。スペースを使用して、ネットワーク マスク、および後続の IP アドレスとネットワーク マスクのペアを区切ります。
tunnel	社内ネットワークから Easy VPN クライアントとして動作している ASA 5505 の外部インターフェイスへの管理アクセス専用 IPsec トンネルを自動的に設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

ASA 5505 のコンフィギュレーションに次のコマンドが含まれていることを前提とします。

- **vpnclient server**：ピアを指定します。
- **vpnclient mode**：クライアントモード（PAT）またはネットワーク拡張モードを指定します。

次のいずれかです。

- **vpnclient vpngroup**：Easy VPN サーバーで認証に使用するトンネルグループと IKE 事前共有キーを指定します。
- **vpnclient trustpoint**：認証に使用する RSA 証明書を識別するトラストポイントを指定します。

（注） NAT デバイスでスタティック NAT マッピングを追加しなければ、NAT デバイスの背後にある ASA のパブリック アドレスにはアクセスできません。

（注） コンフィギュレーションにかかわらず、DHCP 要求（更新メッセージを含む）は IPSec トンネル上を流れません。vpnclient management tunnel を使用しても、DHCP トラフィックは許可されません。

例

次に、ASA 5505 の外部インターフェイスから IP アドレスとマスクの組み合わせが 192.168.10.10 255.255.255.0 であるホストへの IPsec トンネルを生成する例を示します。

```
ciscoasa
(config)#
vpnclient management tunnel 192.168.10.0 255.255.255.0
ciscoasa
(config)#
```

次に、IPsec を使用しないで ASA 5505 の外部インターフェイスへの管理アクセスを提供する例を示します。

```
ciscoasa(config)# vpnclient management clear
ciscoasa(config)#
```

vpnclient mode

クライアントモードまたはネットワーク拡張モードの Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient mode** 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この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。

vpnclient mode { **client-mode | network-extension-mode** }
no vpnclient mode

構文の説明

client-mode	クライアント モード（PAT）を使用するように Easy VPN Remote 接続を設定します。
network-extension-mode	ネットワーク拡張モード（NEM）を使用するように Easy VPN Remote 接続を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

Easy VPN クライアントは、クライアント モードまたは NEM のいずれかの動作モードをサポートします。動作モードによって、企業ネットワークからトンネル経由で内部ホスト（Easy VPN クライアントから見た場合の内部ホスト）に接続できるかどうかが決まります。Easy VPN クライアントにはデフォルト モードがないため、接続前に動作モードを指定する必要があります。

- クライアント モードでは、Easy VPN クライアントは、内部ホストからのすべての VPN トラフィックに対してポート アドレス変換（PAT）を実行します。このモードでは、ハード

ウェア クライアント（デフォルトの RFC 1918 アドレスが割り当てられています）の内部アドレスまたは内部ホストに対する IP アドレス管理は必要ありません。PAT により、企業ネットワークから内部ホストにはアクセスできません。

- NEM では、内部ネットワーク上のすべてのノードおよび内部インターフェイスに企業ネットワークでルーティング可能なアドレスが割り当てられます。内部ホストには、企業ネットワークからトンネル経由でアクセスできます。内部ネットワーク上のホストには、アクセス可能なサブネットから IP アドレスが（スタティックに、または DHCP によって）割り当てられます。ネットワーク拡張モードの場合、PAT は VPN トラフィックに適用されません。

（注） Easy VPN ハードウェアクライアントが NEM を使用し、セカンダリサーバーに接続している場合は、各ヘッドエンドデバイスで **crypto map set reverse-route** コマンドを使用して、逆ルート注入（RRI）によるリモートネットワークのダイナミック通知を設定します。

例

次に、クライアント モードの Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa
(config)#
vpnclient mode client-mode
ciscoasa
(config)#
```

次に、NEM の Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa
(config)#
vpnclient mode network-extension-mode
ciscoasa
(config)#
```

vpnclient nem-st-autoconnect

NEM およびスプリットトンネリングが設定されている場合に、IPsec データトンネルを自動的に開始するように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient nem-st-autoconnect** 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この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。

vpnclient nem-st-autoconnect
no vpnclient nem-st-autoconnect

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

vpnclient nem-st-autoconnect コマンドを入力する前に、ハードウェアクライアントのネットワーク拡張モードがイネーブルになっていることを確認します。ネットワーク拡張モードを使用すると、ハードウェア クライアントは、単一のルーティング可能なネットワークを VPN トンネルを介してリモート プライベート ネットワークに提供できます。IPsec は、ハードウェアクライアントの背後にあるプライベートネットワークから ASA の背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、ASA の背後にあるデバイスは、ハードウェアクライアントの背後にある、トンネルを介したプライベートネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。ハードウェアクライアントがトンネルを開始する必要があります。トンネルのアップ後、いずれの側からでもデータ交換を開始できます。

（注） ネットワーク拡張モードをイネーブルするようにEasy VPN サーバーを設定する必要もあります。そのためには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。

ネットワーク拡張モードでは、スプリット トンネリングが設定されている場合を除き、IPsec データ トンネルが自動的に開始し、保持されます。

例

次に、スプリット トンネリングが設定されたネットワーク拡張モードで自動的に接続するようにEasy VPN Remote接続を設定する例を示します。グループ ポリシーFirstGroupのネットワーク拡張モードがイネーブルになっています。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)
# nem enable
ciscoasa
(config)#
vpnclient nem-st-autoconnect
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
nem	ハードウェア クライアントのネットワーク拡張モードをイネーブルにします。

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。

no vpnclient sercure interface

vpnclient server

Easy VPN Remote 接続用のプライマリおよびセカンダリ IPsec サーバーを設定するには、グローバル コンフィギュレーション モードで **vpnclient 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この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。

vpnclient server *ip_primary_address* [*ip_secondary_address_1 … ipsecondary_address_10*]
no vpnclient server

構文の説明

ip_primary_address	プライマリ Easy VPN（IPsec）サーバーの IP アドレスまたは DNS 名。ASA または VPN 3000 コンセントレータ シリーズは、Easy VPN サーバーとして機能できます。
ip_secondary_address_n	（任意）最大 10 台のバックアップ Easy VPN サーバーの IP アドレスまたは DNS 名のリスト。スペースを使用して、リスト内の項目を区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

接続を確立する前にサーバーを設定する必要があります。**vpnclient server** コマンドでは、IPv4 アドレス、名前データベース、または DNS 名がサポートされ、アドレスはこの順序で解決されます。

サーバーの IP アドレスまたはホスト名を使用できます。

例

次に、名前 headend-1 をアドレス 10.10.10.10 に関連付け、**vpnclient server** コマンドを使用して 3 台のサーバー（headend-dns.example.com（プライマリ）、headend-1（セカンダリ）、および 192.168.10.10（セカンダリ））を指定する例を示します。

```
ciscoasa
(config)#
names
ciscoasa(config)# 10.10.10.10 headend-1
ciscoasa(config)# vpnclient server headend-dns.example.com headend-1 192.168.10.10
ciscoasa(config)#
```

次に、VPN クライアントに IP アドレスが 10.10.10.15 のプライマリ IPsec サーバーおよび IP アドレスが 10.10.10.30 と 192.168.10.45 のセカンダリ サーバーを設定する例を示します。

```
ciscoasa
(config)#
vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
ciscoasa
(config)#
```

vpnclient server-certificate

証明書マップによって指定された特定の証明書を持つ Easy VPN サーバーへの接続のみを受け入れるように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient server-certificate** 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この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。

vpnclient server-certificate *certmap_name*
no vpnclient server-certificate

構文の説明

certmap_name	受け入れ可能な Easy VPN サーバー証明書を指定する証明書マップの名前を指定します。最大長は、64 文字です。

コマンド デフォルト

Easy VPN サーバー証明書のフィルタリングは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

このコマンドを使用して、Easy VPN サーバー証明書のフィルタリングをイネーブルにします。証明書マップ自体は、crypto ca certificate map コマンドと crypto ca certificate chain コマンドを使用して定義します。

例

次に、homeservers という名前の証明書マップを持つ Easy VPN サーバーへの接続のみをサポートするように Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa
(config)#
```

```
vpnclient server-certificate homeservers
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
certificate	指定された証明書を追加します。
vpnclient trustpoint	Easy VPN Remote 接続で使用する RSA アイデンティティ証明書を設定します。

vpnclient trustpoint

Easy VPN Remote 接続で使用する RSA アイデンティティ証明書を設定するには、グローバル コンフィギュレーション モードで **vpnclient trustpoint** 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この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。

vpnclient trustpoint *trustpoint_name* [**chain**]
no vpnclient trustpoint

構文の説明

chain	証明書チェーン全体を送信します。
trustpoint_name	認証に使用する RSA 証明書を識別するトラストポイントの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

crypto ca trustpoint コマンドを使用してトラストポイントを定義します。トラストポイントは、CA が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。トラストポイントサブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。これらのパラメータでは、ASA が CA 証明書を取得する方法、ASA が CA から証明書を取得する方法、および CA が発行するユーザー証明書の認証ポリシーを指定します。

例

次に、central という名前の特定のアイデンティティ証明書を使用し、証明書チェーン全体を送信するように Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint
central
ciscoasa
(config)#
vpnclient trustpoint central chain
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのトラストポイントサブモードを開始し、トラストポイント情報を管理します。

vpnclient username

Easy VPN Remote 接続の VPN ユーザー名とパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient username** 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この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。

vpnclient username *xauth_username* **password** *xauth password*
no vpnclient username

構文の説明

xauth_password	XAUTH に使用するパスワードを指定します。最大長は、64 文字です。
xauth_username	XAUTH に使用するユーザー名を指定します。最大長は、64 文字です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

XAUTHユーザー名とパスワードのパラメータは、セキュアユニット認証がディセーブルで、サーバーがXAUTHクレデンシャルを要求する場合に使用します。セキュアユニット認証がイネーブルの場合、これらのパラメータは無視され、ASAによって、ユーザー名とパスワードの入力を求めるプロンプトが表示されます。

例

次に、XAUTH ユーザー名 testuser とパスワード ppurkm1 を使用するように Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa
```

```
(config)#
vpnclient username testuser password ppurkm1
ciscoasa
(config)#
```

vpnclient vpngroup

Easy VPN Remote 接続の VPN トンネルグループ名とパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient vpngroup** 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この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。

vpnclient vpngroup *group_name* **password** *preshared_key*
no vpnclient vpngroup

構文の説明

group_name	Easy VPN サーバーで設定された VPN トンネル グループの名前を指定します。最大の長さは 64 文字で、スペースは使用できません。
preshared_key	Easy VPN サーバーで認証に使用する IKE 事前共有キー。最大長は 128 文字です。

コマンド デフォルト

Easy VPN Remote ハードウェア クライアントとして動作している ASA の設定でトンネル グループが指定されていない場合、クライアントは RSA 証明書を使用しようとします。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

事前共有キーをパスワードとして使用します。

また、接続を確立する前に、サーバーを設定してモードを指定する必要もあります。

例

次に、グループ名が TestGroup1、パスワードが my_key123 の VPN トンネル グループを Easy VPN Remote 接続に設定する例を示します。

```
ciscoasa
(config)#
vpnclient vpngroup TestGroup1 password my_key123
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
vpnclient trustpoint	Easy VPN 接続で使用する RSA アイデンティティ証明書を設定します。

vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グローバルポリシーまたはユーザー名モードで **vpn-filter** コマンドを使用します。**vpn-filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループポリシーから継承できるようになります。値が継承されないようにするには、**vpn-filter none** コマンドを使用します。

このユーザーまたはグループポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。次に、**vpn-filter** コマンドを使用して、それらの ACL を適用します。

vpn-filter { **value** *ACL name* **| none** }
no vpn-filter

構文の説明

none	アクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACL name*	事前に設定済みのアクセス リストの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	• 対応	—
ユーザー名コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
9.0(1)	IPv4 および IPv6 ACL のサポートが追加されました。マルチ コンテキスト モードのサポートが追加されました。
9.1.(4)	IPv4 および IPv6 ACL のサポートが追加されました。廃止されたコマンド **ipv6-vpn-filter** が IPv6 ACL を指定するために誤って使用された場合、接続は終了します。

使用上のガイドライン

クライアントレス SSL VPN では、**vpn-filter** コマンドで定義された ACL は使用されません。

設計上、vpn-filter 機能では、インバウンド方向のトラフィックだけにフィルタを適用できます。アウトバウンド ルールは自動的にコンパイルされます。icmp アクセス リストを作成するときに、方向フィルタを適用する場合は、アクセス リスト形式で icmp タイプを指定しないでください。

VPN フィルタは初期接続にのみ適用されます。アプリケーション インスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。

例

次に、FirstGroup という名前のグループ ポリシーの、acl_vpn というアクセス リストを呼び出すフィルタを設定する例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-filter value acl_vpn
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
ipv6-vpn-filter	以前は IPv6 ACL を指定するために使用された廃止されたコマンドです。

vpn-framed-ip-address

個々のユーザーに割り当てる IPv4 アドレスを指定するには、ユーザー名モードで **vpn-framed-ip-address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip-address { *ip_address* }{ *subnet_mask* }
no vpn-framed-ip-address

構文の説明

ip_address	このユーザーの IP アドレスを指定します。
subnet_mask	サブネットワーク マスクを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、anyuser という名前のユーザーに IP アドレス 10.92.166.7 を設定する例を示します。

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)#
vpn-framed-ip-address 10.92.166.7 255.255.255.254
```

vpn-framed-ipv6-address

ユーザーに専用のIPv6アドレスを割り当てるには、ユーザー名モードで**vpn-framed-ipv6-address**コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip6-address *ip_address/subnet_mask*
no vpn-framed-ip6-address *ip_address/subnet_mask*

構文の説明

ip_address	このユーザーのIPアドレスを指定します。
subnet_mask	サブネットワーク マスクを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、*anyuser* という名前のユーザーに IP アドレスとネットマスク 2001::3000:1000:2000:1/64 を設定する例を示します。このアドレスは、プレフィックス値 2001:0000:0000:0000 およびインターフェイス ID 3000:1000:2000:1 を示しています。

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)#
vpn-framed-ipv6-address
2001::3000:1000:2000:1/64
ciscoasa(config-username)
```

関連コマンド

コマンド	説明
vpn-framed-ip-address	個々のユーザーに割り当てる IPv4 アドレスを指定します。

vpn-group-policy

ユーザーが設定済みのグループポリシーから属性を継承するようにするには、ユーザー名コンフィギュレーションモードでvpn-group-policyコマンドを使用します。グループポリシーをユーザー 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。このコマンドを使用すると、ユーザーはユーザー名レベルで設定されていない属性を継承できます。

vpn-group-policy { *group-policy name* }
no vpn-group-policy { *group-policy name* }

構文の説明

group-policy name	グループポリシーの名前を指定します。

コマンド デフォルト

デフォルトでは、VPN ユーザーにはグループ ポリシーが関連付けられません。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

特定ユーザーのグループポリシーの属性値を上書きするには、その値をユーザー名モードで設定します（その属性をユーザー名モードで使用できる場合）。

例

次に、FirstGroup という名前のグループ ポリシーから属性を使用するように anyuser という名前のユーザーを設定する例を示します。

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)# vpn-group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループポリシーを ASA データベースに追加します。
group-policy attributes	グループ ポリシー属性モードを開始します。これにより、グループ ポリシーの AVP を設定できます。
username	ASA データベースにユーザーを追加します。
username attributes	ユーザー名属性モードを開始します。これにより、特定のユーザーの AVP を設定できます。

vpn-idle-timeout

ユーザータイムアウト期間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを使用します。この期間中に接続上で通信アクティビティがない場合、ASA は接続を終了します。任意で、タイムアウトのアラート間隔をデフォルトの 1 分から延長できます。

実行コンフィギュレーションからこの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、他のグループポリシーからタイムアウト値を継承できます。値が継承されないようにするには、**vpn-idle-timeout none** コマンドを使用します。

vpn-idle-timeout { *minutes* **| none** } [**alert-interval** *minutes*]
no vpn-idle-timeout
no vpn-idle-timeout alert-interval

構文の説明

minutes	タイムアウト期間の分数、およびタイムアウト アラートまでの分数を指定します。1 ～ 35791394 の整数を使用します。
none	AnyConnect（SSL IPsec/IKEv2）：次のコマンドで設定されたグローバル WebVPN default-idle-timeout 値（秒単位）を使用します。ciscoasa**(config-webvpn)# default-idle-timeout** WebVPN **default-idle-timeout** コマンドにおけるこの値の範囲は、60 ～ 86400 秒です。デフォルトのグローバル WebVPN アイドルタイムアウト（秒単位）は、1800 秒（30 分）です。 （注） すべての AnyConnect 接続では、ASA によってゼロ以外のアイドル タイムアウト値が要求されます。 WebVPN ユーザーの場合、**default-idle-timeout** 値は、vpn-idle-timeout none がグループポリシー/ユーザー名属性に設定されている場合にのみ有効です。 サイト間（IKEv1、IKEv2）および IKEv1 リモートアクセス：タイムアウトをディセーブルにし、無制限のアイドル期間を許可します。

コマンド デフォルト

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

セキュアクライアント は、SSL および IKEv2 接続のセッション再開をサポートします。この機能により、エンドユーザー デバイスはスリープ モードに移行し、WiFi または同様の接続を失い、戻り時に同じ接続を再開できます。

例

次の例は、「FirstGroup」という名前のグループ ポリシーに 15 分の VPN アイドル タイムアウトを設定する方法を示しています。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-idle-timeout 30
```

セキュリティ アプライアンスは、vpn-idle-timeout 値が 0 の場合、または値が有効な範囲に該当しない場合にユーザーに対して値が定義されていない場合、default-idle-timeout 値を使用します。

関連コマンド

default-idle-timeout	グローバル WebVPN デフォルト アイドル タイムアウトを指定します。
group-policy	グループ ポリシーを作成または編集します。
vpn-session-timeout	VPN 接続の最大許容時間を設定します。この期間が終了すると、ASA は接続を終了します。

vpn ロード バランシング

VPN ロードバランシングおよび関連機能を設定できる VPN ロードバランシング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 **vpn load-balancing** コマンドを使用します。

vpn load-balancing

（注） VPN ロードバランシングを使用するには、Plus ライセンス付きの ASA 5510、または ASA 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	ASA 5510（Plus ライセンス付き）および 5520 以降のモデルのサポートが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ロードバランシング クラスタには、セキュリティ アプライアンス モデル 5510（Plus ライセンス付き）または ASA 5520 以降を含めることができます。VPN 3000 シリーズのコンセントレータも含めることができます。混合コンフィギュレーションは可能ですが、通常は、同種クラスタにする方が容易に管理できます。

vpn load-balancing コマンドを使用して、VPN ロード ランシングモードを開始します。VPN ロード バランシング モードでは、次のコマンドを使用できます。

- **cluster encryption**
- **cluster ip address**
- **cluster key**
- **cluster port**
- **interface**
- **nat**
- **participate**
- **priority**
- **redirect-fqdn**

詳細については、個々のコマンドの説明を参照してください。

例

次に、**vpn load-balancing** コマンドの例を示します。プロンプトが変わる点に注意してください。

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)#
```

次に、interface コマンドを含む VPN load-balancing コマンド シーケンスの例を示します。interface コマンドでは、クラスタのパブリック インターフェイスを「test」、クラスタのプライベート インターフェイスを「foo」と指定しています。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
```

ciscoasa(config-load-balancing)# **participate**

関連コマンド

コマンド	説明
clear configure vpn load-balancing	ロード バランシングの実行時コンフィギュレーションを削除し、ロード バランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示します。
show vpn load-balancing	VPN ロード バランシング実行時の統計情報を表示します。

vpn-sessiondb

VPN セッションまたは セキュアクライアント VPN セッションの最大数を指定するには、グローバル コンフィギュレーション モードで vpn-sessiondb コマンドを使用します。コンフィギュレーションから制限を削除するには、このコマンドの no 形式を使用します。

vpn-sessiondb { **max-anyconnect-premium-or-essentials-limit** *number* | **max-other-vpn-limit** *number* }

構文の説明

max-anyconnect-premium-or-essentials-limit number	AnyConnect セッションの最大数を指定します（1 ～ ライセンスで許可される最大セッションまで）。
max-other-vpn-limit number	セキュアクライアント セッション以外の VPN セッションの最大数（1 からライセンスで許可される最大セッション数）を指定します。これには、Cisco VPN Client（IPsec IKEv1）および LAN-to-LAN VPN が含まれます。

コマンド デフォルト

デフォルトでは、ASA は VPN セッション数をライセンスで許可される最大数未満に制限しません。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	次のキーワードが変更されました。 • max-anyconnect-premium-or-essentials-limit replaced max-session-limit • max-other-vpn-limit replaced max-webvpn-session-limit
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、最大 AnyConnect セッションを 200 に設定する例を示します。

```
ciscoasa(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 200
```

関連コマンド

コマンド	説明
vpn-sessiondb logoff	すべて、または特定のタイプの IPSec VPN セッションおよび WebVPN セッションをログオフします。
vpn-sessiondb max-webvpn-session-limit	WebVPN セッションの最大数を設定します。

vpn-sessiondb logoff

すべてのVPNセッションまたは選択したVPNセッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff** コマンドを使用します。

vpn-sessiondb logoff { **all | anyconnect | email-proxy | index index_number | ipaddress** *IPaddr* **| l2l | name** *username* **| protocol** *protocol-name* **| ra-ikev1-ipsec | ra-ikev2-ipsec | tunnel-group** *groupname* **| vpn-lb | webvpn** }[**noconfirm**]

構文の説明

all	すべての VPN セッションをログオフします。
anyconnect	すべての AnyConnect VPN クライアント セッションをログオフします。
email-proxy	（廃止）すべての電子メール プロキシ セッションをログオフします。
index *index_number*	インデックス番号で 1 つのセッションをログオフします。セッションのインデックス番号を指定します。show vpn-sessiondb detail コマンドを使用して、各セッションのインデックス番号を表示できます。
ipaddress *IPaddr*	指定した IP アドレスのセッションをログオフします。
l2l	すべての LAN-to-LAN セッションをログオフします。
name *username*	指定したユーザー名のセッションをログオフします。
protocol *protocol-name*	指定したプロトコルのセッションをログオフします。プロトコルは次のとおりです。

	• ikev1：インターネット キー交換バージョン 1（IKEv1）プロトコルを使用するセッション。 • ikev2：インターネット キー交換バージョン 2（IKEv2）プロトコルを使用するセッション。 • ipsec：IKEv1 または IKEv2 を使用した IPsec セッション。 • ipseclan2lan：IPsec LAN-to-LAN セッション。 • ipseclan2lanovernatt：IPsec LAN-to-LAN over NAT-T セッション。 • ipsecovernatt：IPsec over NAT-T セッション。 • ipsecovertcp：IPsec over TCP セッション。 • ipsecoverudp：IPsec over UDP セッション。 • l2tpOverIpSec：L2TP over IPsec セッション。 • l2tpOverIpsecOverNatT：NAT-T を介した L2TP over IPsec セッション。 • webvpn：クライアントレス SSL VPN セッション。 • imap4s：IMAP4 セッション。 • pop3s：POP3 セッション。 • smtps：SMTP セッション。 • anyconnectParent：セキュアクライアント セッション。セッションに使用されるプロトコルに関係なく、AnyConnect IPsec IKEv2 セッションおよび SSL セッションを終了します。 • ssltunnel：SSL を使用した AnyConnect セッションやクライアントレス SSL VPN セッションを含めた、SSL VPN セッション。 • dtlstunnel：DTLS が有効になっている セキュアクライアント セッション。
ra-ikev1-ipsec	すべての IPsec IKEv1 リモート アクセス セッションをログオフします。
ra-ikev2-ipsec	すべての IPsec IKEv2 リモート アクセス セッションをログオフします。
tunnel-group *groupname*	指定したトンネル グループ（接続プロファイル）のセッションをログオフします。
webvpn	すべてのクライアントレス SSL VPN セッションをログオフします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	次の protocol キーワードが変更または追加されました。 • remote が ra-ikev1-ipsec に変更されました。 • ike が ikev1 に変更されました。 • ikev2 が追加されました。 • anyconnectParent が追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.3(2)	**ra-ikev2-ipsec** キーワードが追加されました。
9.8(1)	**email-proxy** オプションが廃止されました。

例

次に、すべての セキュアクライアント セッションをログオフする例を示します。

```
ciscoasa# vpn-sessiondb logoff anyconnect
```

次に、すべての IPsec セッションをログオフする例を示します。

```
ciscoasa# vpn-sessiondb logoff protocol IPsec
```

vpn-session-timeout

VPN 接続に許可される最大時間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用します。この期間が終了すると、ASA は接続を終了します。任意で、タイムアウトのアラート間隔をデフォルトの 1 分から延長できます。

実行コンフィギュレーションからこの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、他のグループ ポリシーからタイムアウト値を継承できます。値が継承されないようにするには、**vpn-session-timeout none** コマンドを使用します。

vpn-session-timeout { *minutes* | **none** } [**alert-interval** *minutes*]
no vpn-session-timeout
no vpn-session-timeout alert-interval

構文の説明

minutes	タイムアウト期間の分数、およびタイムアウト アラートまでの分数を指定します。1 ～ 35791394 の整数を使用します。
none	無制限のセッション タイムアウト期間を許可します。セッション タイムアウトにヌル値を設定して、セッション タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
9.7(1)	**alert-interval** が AnyConnect VPN に適用されました。

例

次に、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-session-timeout 180
```

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-idle-timeout	ユーザー タイムアウト期間を設定します。この期間中に接続上で通信アクティビティがない場合、ASA は接続を終了します。

vpnsetup

ASA で VPN 接続を設定するための手順のリストを表示するには、グローバル コンフィギュレーション モードで **vpnsetup** コマンドを使用します。

vpnsetup { **ipsec-remote-access | l2tp-remote-access | site-to-site | ssl-remote-access** } **steps**

構文の説明

ipsec-remote-access	IPSec 接続を受け入れるように ASA を設定するための手順を表示します。
l2tp-remote-access	L2TP 接続を受け入れるように ASA を設定するための手順を表示します。
site-to-site	LAN-to-LAN 接続を受け入れるように ASA を設定するための手順を表示します。
ssl-remote-access	SSL 接続を受け入れるように ASA を設定するための手順を表示します。
steps	接続タイプの手順を表示することを指定します。

コマンド デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次の例は、**vpnsetup ssl-remote-access steps command:** の出力を示しています。

```
ciscoasa(config-t)# vpnsetup ssl-remote-access steps
Steps to configure a remote access SSL VPN remote access connection and AnyConnect with
 examples:
1. Configure and enable interface
 interface GigabitEthernet0/0
  ip address 10.10.4.200 255.255.255.0
```

```
  nameif outside
  no shutdown
 interface GigabitEthernet0/1
  ip address 192.168.0.20 255.255.255.0
  nameif inside
  no shutdown
2. Enable WebVPN on the interface
 webvpn
  enable outside
3. Configure default route
 route outside 0.0.0.0 0.0.0.0 10.10.4.200
4. Configure AAA authentication and tunnel group
 tunnel-group DefaultWEBVPNGroup type remote-access
 tunnel-group DefaultWEBVPNGroup general-attributes
  authentication-server-group LOCAL
5. If using LOCAL database, add users to the Database
 username test password t3stP@ssw0rd
 username test attributes
  service-type remote-access
Proceed to configure AnyConnect VPN client:
6. Point the ASA to an AnyConnect image
 webvpn
  svc image anyconnect-win-2.1.0148-k9.pkg
7. enable AnyConnect
 svc enable
8. Add an address pool to assign an ip address to the AnyConnect client
 ip local pool client-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
9. Configure group policy
 group-policy DfltGrpPolicy internal
 group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol svc webvpn
ciscoasa(config-t)#
```

関連コマンド

コマンド	説明
show running-config	ASA の実行コンフィギュレーションを表示します。

vpn-simultaneous-logins

ユーザーに許可される同時ログイン数を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用します。属性を削除して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。

vpn-simultaneous-logins *integer*
no vpn-simultaneous-logins

構文の説明

integer	0 ～ 2147483647 の数字。

コマンド デフォルト

デフォルトの同時ログイン数は、3 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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。ログインをディセーブルにしてユーザーのアクセスを禁止するには、0 を入力します。

（注） 同時ログイン数の最大制限は非常に大きい値ですが、複数の同時ログインを許可すると、セキュリティが侵害されたり、パフォーマンスが低下したりすることがあります。

失効したAnyConnect、IPsecクライアント、またはクライアントレスセッション（異常終了したセッション）は、同じユーザー名で「新しい」セッションが確立されても、セッションデータベースに残る場合があります。

vpn-simultaneous-loginsの値が1の場合は、異常終了後に同じユーザーが再度ログインすると、失効したセッションはデータベースから削除され、新しいセッションが確立されます。ただし、既存のセッションがまだアクティブな接続である場合は、同じユーザーが別のPCなどから再度ログインすると、最初のセッションがログオフし、データベースから削除されて、新しいセッションが確立されます。

同時ログイン数が1より大きい値の場合、その最大数に達した状態で再度ログインしようとすると、最もアイドル時間の長いセッションがログオフします。現在のすべてのセッションが同じくらい長い間アイドル状態の場合は、最も古いセッションがログオフします。このアクションにより、セッションが解放されて新しいログインが可能になります。

最大セッション制限に達すると、システムが最も古いセッションを削除するまでに時間がかかります。そのため、ユーザーはすぐにログオンできず、削除が正常に完了する前に新しい接続を再試行する必要が生じる場合があります。ユーザーが想定どおりにログオフした場合、これは問題になりません。必要に応じて、**vpn-simultaneous-login-delete-no-delay**コマンドを使用して、削除が完了するのを待たずにすぐに新しいユーザー接続を許可するようにシステムを設定することで、遅延を解消できます。

例

次に、FirstGroupという名前のグループポリシーに対して最大4つの同時ログインを許可する例を示します。

```
ciscoasa(config)#  group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

VPN トンネルタイプ（IKEv1 または IKEv2 による IPsec、あるいは IPsec、SSL、またはクライアントレス SSL を介した L2TP）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 モードまたはユーザー名コンフィギュレーション モードで **vpn-tunnel-protocol** 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この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。

vpn-tunnel-protocol { **ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless** }
no vpn-tunnel-protocol { **ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless** }

構文の説明

ikev1	2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IKEv1 による IPsec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
ikev2	2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IKEv2 による IPsec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
l2tp-ipsec	L2TP 接続の IPsec トンネルをネゴシエートします。
ssl-client	SSL VPN クライアントについて SSL VPN トンネルをネゴシエートします。
ssl-clientless	HTTPS 対応の Web ブラウザ経由でリモート ユーザーに VPN サービスを提供します。クライアントは必要ありません。

コマンド デフォルト

デフォルトは IPsec 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.17(1)	クライアントレス Web VPN のサポートが削除されたため、ssl-clientless キーワードが削除されました。
8.4(1)	ipsec キーワードは ikev1 および ikev2 キーワードに置き換えられました。
7.3(1)	**svc** キーワードが追加されました。
7.2(1)	**l2tp-ipsec** キーワードが追加されました。
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザーには、少なくとも 1 つのトンネリング モードを設定する必要があります。

（注） IPsec から SSL へのフォールバックをサポートするには、**vpn-tunnel-protocol** コマンドに **svc** 引数と **ipsec** 引数の両方を設定する必要があります。

例

次に、「FirstGroup」という名前のグループ ポリシーに対して WebVPN トンネリング モードと IPsec トンネリング モードを設定する例を示します。

```
ciscoasa
(config)#

group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-tunnel-protocol webvpn
ciscoasa
(config-group-policy)#
 vpn-tunnel-protocol IPsec
```

関連コマンド

コマンド	説明
address pools	アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定します。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

vtep-nve

VXLAN VNI インターフェイスと VTEP 送信元インターフェイスを関連付けるには、インターフェイス コンフィギュレーション モードで **vtep-nve** コマンドを使用します。関連付けを削除するには、このコマンドの **no** 形式を使用します。

vtep-nve 1
no vtep-nve 1

構文の説明

1	NVE インスタンスを指定します（常に 1）。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。この VTEP 送信元インターフェイスを指定する NVE インスタンスを 1 つ設定できます。すべての VNI インターフェイスはこの NVE インスタンスに関連付けられている必要があります。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、VNI 1 インターフェイスをそれに関連付ける例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
```

```
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

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

コマンド	説明
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

vxlan ポート

VXLAN UDP ポートを設定するには、グローバル コンフィギュレーション モードで **vxlan port** コマンドを使用します。デフォルトポートに戻すには、このコマンドの **no** 形式を使用します。

vxlan port *udp_port*
no vxlan port *udp_port*

構文の説明

udp_port	VXLAN UDP ポートを設定します。デフォルト値は 4789 です。

コマンド デフォルト

デフォルト ポートは 4789 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Nve コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。ネットワークで標準以外のポートを使用する場合は、それを変更できます。

例

次に例を示します。

```
ciscoasa(config)# vxlan port 5678
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。