



## 全般 VPN パラメータ

バーチャルプライベートネットワークの ASA の実装には、カテゴリの枠を越えた便利な機能があります。この章では、これらの機能のいくつかについて説明します。

- [注意事項と制約事項 \(1 ページ\)](#)
- [ACL をバイパスするための IPsec の設定 \(2 ページ\)](#)
- [インターフェイス内トラフィックの許可 \(ヘアピンング\) \(3 ページ\)](#)
- [アクティブな IPsec セッションまたは SSL VPN セッションの最大数の設定 \(4 ページ\)](#)
- [許可される IPsec クライアント リビジョンレベル確認のためのクライアントアップデートの使用 \(5 ページ\)](#)
- [パブリック IP 接続への NAT 割り当てによる IP アドレスの実装 \(7 ページ\)](#)
- [VPN セッション制限の設定 \(9 ページ\)](#)
- [ID 証明書のネゴシエート時の使用 \(11 ページ\)](#)
- [暗号化コアのプールの設定 \(11 ページ\)](#)
- [ダイナミック スプリット トンネリングの設定 \(12 ページ\)](#)
- [アクティブな VPN セッションの表示 \(13 ページ\)](#)
- [ISE ポリシー適用について \(16 ページ\)](#)
- [SSL の詳細設定 \(21 ページ\)](#)
- [永続的 IPsec トンネルフロー \(26 ページ\)](#)

## 注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

### コンテキストモードのガイドライン

シングルコンテキストモードとマルチコンテキストモードでサポートされています。『[ASA General Operations CLI Configuration Guide](#)』の適切なリリースでは、マルチコンテキストモードでサポートされていないもののリストについては『[Guidelines for Multiple Context Mode](#)』を参照してください。また「[New Features](#)」には、リリースを通して追加されたものの明細が示されています。

### ファイアウォール モードのガイドライン

ルーテッドファイアウォール モードでだけサポートされています。トランスペアレント モードはサポートされていません。

## ACL をバイパスするための IPsec の設定

IPsec トンネルから送信されるすべてのパケットに対して、ACL で発信元インターフェイスと宛先インターフェイスをチェックせずに許可するには、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを入力します。

IPsec トラフィックのインターフェイス ACL をバイパスする必要があるのは、ASA の背後で別の VPN コンセントレータを使用し、なおかつ ASA のパフォーマンスを最大限にする場合などです。通常、IPsec パケットを許可する ACL を **access-list** コマンドを使用して作成し、これを発信元インターフェイスに適用します。ACL を使用すると、ASA を通過できるトラフィックを正確に指定できます。

次の例では、ACL をチェックせずに ASA を通過する IPsec トラフィックをイネーブルにします。

```
hostname(config)# sysopt connection permit-vpn
```



(注) **no sysopt connection permit-vpn** が設定されているときに、外部インターフェイスのアクセスグループが **deny ip any any** ACL を呼び出すように設定されていたとしても、クライアントからの復号化された通過トラフィックは許可されます。

保護されたネットワークへの、サイトツーサイトまたはリモート アクセス VPN 経由でのアクセスをコントロールするために、**no sysopt permit-vpn** コマンドを外部インターフェイス上のアクセス コントロール リスト (ACL) と組み合わせて使用しようとしても、うまくいきません。

**sysopt connection permit-vpn** は、その対象のトラフィックの暗号マップが有効になっているインターフェイスに対する ACL (インとアウトの両方) と、他のすべてのインターフェイスの出力 (アウト) ACL (入力 (イン) ACL ではない) をバイパスします。

このような状況では、内部の管理アクセスがイネーブルになっていると、ACL は適用されず、ユーザは SSH を使用して ASA に引き続き接続できます。内部ネットワーク上へのホストへのトラフィックは ACL によって正しくブロックされますが、内部インターフェイスへの復号化された通過トラフィックはブロックされません。

**ssh** および **http** コマンドは、ACL よりもプライオリティが高くなります。VPN セッションからボックスへの SSH、Telnet、または ICMP トラフィックを拒否するには、**ssh**、**telnet**、および **icmp** コマンドを使用します。

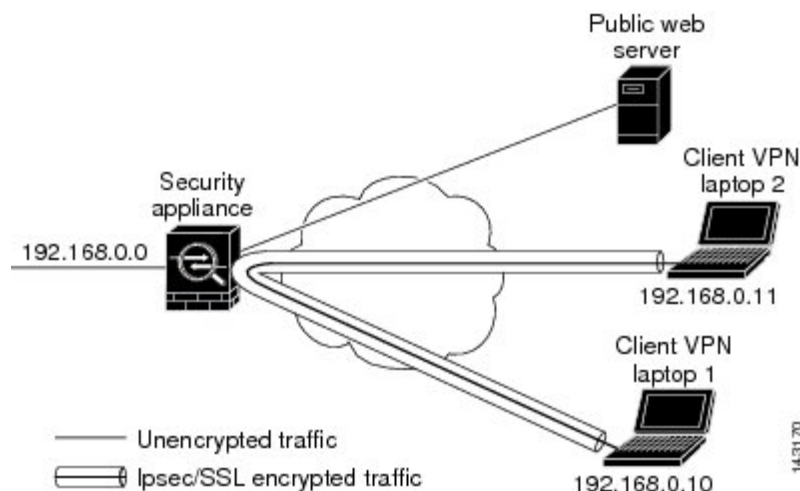
## インターフェイス内トラフィックの許可（ヘアピニング）

ASA には、IPsec で保護されたトラフィックに対して、同じインターフェイスの出入りを許可することにより、VPN クライアントが別の VPN ユーザに IPsec で保護されたトラフィックを送信できる機能があります。「ヘアピニング」とも呼ばれるこの機能は、VPN ハブ（ASA）を介して接続している VPN スポーク（クライアント）と見なすことができます。

ヘアピニングにより、着信 VPN トラフィックを同じインターフェイスを介して暗号化されていないトラフィックとしてリダイレクトすることもできます。この機能は、たとえば、スプリットトンネリングがない状態で、VPN へのアクセスと Web のブラウズの両方を行う必要がある VPN クライアントに役立つ可能性があります。

下の図は、VPN クライアント 1 が VPN クライアント 2 に対してセキュアな IPsec トラフィックを送信し、パブリック Web サーバに対しては暗号化されていないトラフィックを送信していることを示しています。

図 1: ヘアピニングにインターフェイス内機能を使用する VPN クライアント



この機能を設定するには、グローバル コンフィギュレーション モードで `intra-interface` 引数を指定して `same-security-traffic permit` コマンドを実行します。

コマンドの構文は、`same-security-traffic permit {inter-interface | intra-interface}` です。

次の例では、インターフェイス内トラフィックをイネーブルにする方法を示しています。

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```



(注) `same-security-traffic` コマンドに `inter-interface` 引数を指定すると、セキュリティ レベルが同一のインターフェイス間の通信が許可されます。この機能は、IPsec 接続に固有のものではありません。詳細については、このマニュアルの「インターフェイスパラメータの設定」の章を参照してください。

ヘアピンングを使用するには、「インターフェイス内トラフィックにおける NAT の注意事項」に記載されているように、適切な NAT ルールを ASA インターフェイスに適用する必要があります。

## インターフェイス内トラフィックにおける NAT の注意事項

ASA がインターフェイスを介して暗号化されていないトラフィックを送信するには、そのインターフェイスに対する NAT をイネーブルにし、プライベート IP アドレスをパブリックにルーティング可能なアドレスに変換する必要があります（ただし、ローカル IP アドレスプールすでにパブリック IP アドレスを使用している場合は除きます）。次の例では、クライアント IP プールから発信されたトラフィックに、インターフェイス PAT ルールを適用しています。

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# object network vpn_nat
hostname(config-network-object)# subnet 192.168.0.0 255.255.255.0
hostname(config-network-object)# nat (outside,outside) interface
```

ただし、ASA がこの同じインターフェイスから暗号化された VPN トラフィックを送信する場合、NAT は任意です。VPN 間ヘアピンングは、NAT を使用してもしなくても機能します。すべての発信トラフィックに NAT を適用するには、上記のコマンドを実装するだけです。VPN 間トラフィックを NAT から免除するには、次のように、VPN 間トラフィックの NAT 免除を実装するコマンドを（上記のコマンドに）追加します。

```
hostname(config)# nat (outside,outside) source static vpn_nat vpn_nat destination static
vpn_nat vpn_nat
```

NAT ルールの詳細については、このマニュアルの「NAT の適用」の章を参照してください。

## アクティブな IPsec セッションまたは SSL VPN セッションの最大数の設定

VPN セッションの数を ASA が許可する数よりも小さい値に制限するには、グローバル コンフィギュレーション モードで `vpn-sessiondb` コマンドを入力します。

```
vpn-sessiondb {max-anyconnect-premium-or-essentials-limit <number> | max-other-vpn-limit
<number>}
```

`max-anyconnect-premium-or-essentials-limit` キーワードは、ライセンスで許可される AnyConnect セッションの最大数を 1 から最大数まで指定します。



(注) 正しいライセンス、用語、階層、およびユーザ数は、これらのコマンドで決定されなくなりました。『AnyConnect Ordering Guide』を参照してください。 <http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf>

**max-other-vpn-limit** キーワードは、ライセンスで許可される（AnyConnect クライアントセッション以外の）VPN セッションの最大数を 1 から最大数まで指定します。これには、Cisco VPN Client（IPsec IKEv1）および LAN-to-LAN VPN セッションが含まれます。

このセッション数の制限は、VPN ロードバランシング用に算出されたロード率に影響します。

次に、最大 Anyconnect VPN セッション数の制限を 450 に設定する例を示します。

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 450
hostname(config)#
```

## 許可される IPsec クライアント リビジョン レベル確認のためのクライアントアップデートの使用



(注) この項の情報は、IPsec 接続にのみ適用されます。

クライアントアップデート機能を使用すると、中央にいる管理者は、VPN クライアントソフトウェアをアップデートする時期を VPN クライアント ユーザに自動的に通知できます。

リモートユーザは、旧式の VPN ソフトウェアバージョンまたはハードウェアクライアントバージョンを使用している可能性があります。**client-update** コマンドを使用すると、いつでもクライアントリビジョンのアップデートをイネーブルにして、アップデートを適用するクライアントのタイプおよびリビジョン番号を指定し、アップデートを取得する URL または IP アドレスを提供できます。また、Windows クライアントの場合は、オプションで、VPN クライアントバージョンをアップデートする必要があることをユーザに通知できます。Windows クライアントに対しては、更新を実行するメカニズムをユーザに提供できます。このコマンドは、IPsec リモートアクセス トンネル グループ タイプにのみ適用されます。

クライアントアップデートを実行するには、一般コンフィギュレーションモードまたはトンネルグループ ipsec 属性コンフィギュレーションモードで **client-update** コマンドを入力します。リビジョン番号のリストにあるソフトウェアバージョンをすでに実行しているクライアントの場合は、ソフトウェアを更新する必要はありません。リストにあるソフトウェアバージョンを実行していないクライアントの場合は、ソフトウェアを更新する必要があります。次の手順は、クライアントアップデートの実行方法を示しています。

### 手順

- ステップ 1** グローバル コンフィギュレーションモードで、次のコマンドを入力してクライアントアップデートをイネーブルにします。

```
hostname(config)# client-update enable
hostname(config)#
```

**ステップ 2** グローバル コンフィギュレーション モードで、特定のタイプのすべてのクライアントに適用するクライアントアップデートのパラメータを指定します。つまり、クライアントのタイプ、アップデートイメージを取得する URL または IP アドレス、および許可されるリビジョン番号または対象クライアントの番号を指定します。最大4つのリビジョン番号をカンマで区切って指定できます。

ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントをアップデートする必要はありません。このコマンドは、ASA 全体にわたって指定されているタイプのすべてのクライアントのクライアントアップデート値を指定します。

次の構文を使用します。

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers
hostname(config)#
```

使用可能なクライアントのタイプは、**win9X** (Windows 95、Windows 98、および Windows ME プラットフォームを含む)、**winnt** (Windows NT 4.0、Windows 2000、および Windows XP プラットフォームを含む)、**windows** (Windows ベースのすべてのプラットフォームを含む) です。

リビジョン番号のリストにあるソフトウェアバージョンをすでに実行しているクライアントの場合は、ソフトウェアを更新する必要はありません。リストにあるソフトウェアバージョンを実行していないクライアントの場合は、ソフトウェアを更新する必要があります。これらのクライアントアップデートエントリから3つまで指定することができます。キーワード **windows** を指定すると、許可されるすべての Windows プラットフォームがカバーされます。**windows** を指定する場合は、個々の Windows クライアントタイプは指定しないでください。

(注) すべての Windows クライアントでは、URL のプレフィックスとしてプロトコル **http://** または **https://** を使用する必要があります。

次の例では、リモートアクセス トンネルグループのクライアントアップデートパラメータを設定しています。リビジョン番号 4.6.1 とアップデートを取得するための URL (**https://support/updates**) を指定します。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

あるいは、特定のタイプのすべてのクライアントではなく、個々のトンネルグループだけのためのクライアントアップデートを設定できます (ステップ 3 を参照)。

(注) URL の末尾にアプリケーション名を含めることで (例: **https://support/updates/vpnclient.exe**)、アプリケーションを自動的に起動するようにブラウザを設定できます。

**ステップ 3** 特定の ipsec-ra トンネルグループの **client-update** パラメータのセットを定義します。

トンネルグループ ipsec 属性モードで、トンネルグループ名とそのタイプ、アップデートされたイメージを取得する URL または IP アドレス、およびリビジョン番号を指定します。ユーザ

のクライアントのリビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合、クライアントをアップデートする必要はありません。たとえば、Windows クライアントの場合、次のコマンドを入力します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

**ステップ 4** (任意) クライアントのアップデートが必要な旧式の Windows クライアントを使用しているアクティブなユーザに通知を送信します。これらのユーザにはポップアップウィンドウが表示され、ブラウザを起動して、URL で指定したサイトからアップデートされたソフトウェアをダウンロードする機会が提供されます。このメッセージで設定可能な部分は URL だけです (ステップ 2 または 3 を参照)。アクティブでないユーザは、次回ログオン時に通知メッセージを受信します。この通知は、すべてのトンネルグループのすべてのアクティブクライアントに送信するか、または特定のトンネルグループのクライアントに送信できます。たとえば、すべてのトンネルグループのすべてのアクティブクライアントに通知する場合は、特権 EXEC モードで次のコマンドを入力します。

```
hostname# client-update all
hostname#
```

ユーザのクライアントのリビジョン番号が指定されているリビジョン番号のいずれかと一致している場合、そのクライアントをアップデートする必要はなく、通知メッセージはユーザに送信されません。

---

#### 次のタスク



(注) クライアント更新のタイプを **windows** (Windows ベースのすべてのプラットフォーム) に指定し、その後、同じエンティティに **win9x** または **winnt** のクライアント更新タイプを入力する必要がある場合は、まずこのコマンドの **no** 形式で **windows** クライアントタイプを削除してから、新しい **client-update** コマンドを使用して新しいクライアントタイプを指定します。

## パブリック IP 接続への NAT 割り当てによる IP アドレスの実装

まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバ

およびネットワークセキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリックアドレスに戻す場合があります。

Cisco ASA 55xx では、内部/保護対象ネットワークの VPN クライアントの割り当てられた IP アドレスをパブリック（送信元）IP アドレスに変換する方法が導入されました。この機能は、内部ネットワークおよびネットワークセキュリティポリシーのターゲットサーバ/サービスが、社内ネットワークの割り当てられた IP ではなく、VPN クライアントのパブリック/送信元 IP との通信を必要とするシナリオをサポートします。

この機能は、トンネルグループごとに1つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。

ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。

- レガシー（IKEv1）クライアントと AnyConnect クライアントだけをサポートします。
- NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターントラフィックは ASA にルーティングされる必要があります。
- 割り当てられた IPv4 およびパブリックアドレスだけをサポートします。
- NAT/PAT デバイスの背後にある複数のピアはサポートされません。
- ロードバランシングはサポートされません（ルーティングの問題のため）。
- ローミングはサポートされません。

## 手順

**ステップ1** グローバル コンフィギュレーション モードで、**tunnel general** を入力します。

**ステップ2** アドレス変換をイネーブルにするには、次の構文を使用します。

```
hostname (config-tunnel-general)# nat-assigned-to-public-ip interface
```

このコマンドは、送信元のパブリック IP アドレスに、割り当てられた IP アドレスの NAT ポリシーをダイナミックにインストールします。*interface* は、NAT の適用先を決定します。

**ステップ3** アドレス変換をディセーブルにするには、次の構文を使用します。

```
hostname (config-tunnel-general)# no nat-assigned-to-public-ip
```

## VPN NAT ポリシーの表示

アドレス変換は、基礎となるオブジェクト NAT メカニズムを使用します。そのため、VPN NAT ポリシーは、手動設定されたオブジェクト NAT ポリシーと同様に表示されます。次の例



では、割り当てられた IP として 95.1.226.4 を使用して、ピアのパブリック IP として 75.1.224.21 を使用します。

```
hostname# show nat
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
   translate_hits = 315, untranslate_hits = 315

prompt# show nat detail

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
   translate_hits = 315, untranslate_hits = 315
   Source - Origin: 95.1.226.4/32, Translated: 75.1.224.21/32
```

*outside* は AnyConnect クライアントが接続するインターフェイスであり、*inside* は新しいトンネルグループに固有のインターフェイスです。



(注) VPN NAT ポリシーがダイナミックであり、設定に追加されないため、VPN NAT オブジェクトおよび NAT ポリシーは、`show run object` レポートおよび `show run nat` レポートから非表示になります。

## VPN セッション制限の設定

IPsec セッションと SSL VPN セッションは、プラットフォームと ASA ライセンスがサポートする限り、いくつでも実行できます。ASA の最大セッション数を含むライセンス情報を表示するには、グローバル コンフィギュレーション モードで `show version` コマンドを入力し、ライセンスのセクションを探します。次の例は、このコマンドの出力からのコマンドとライセンスの情報を示しています。もう一方の出力は明確にするために編集されています。

```
hostname(config)# show version
...
Licensed features for this platform:
Maximum Physical Interfaces      : Unlimited      perpetual
Maximum VLANs                  : 500           perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Active perpetual
Encryption-DES                  : Enabled       perpetual
Encryption-3DES-AES            : Enabled       perpetual
Security Contexts               : 100          perpetual
Carrier                         : Enabled       perpetual
AnyConnect Premium Peers       : 5000         perpetual
AnyConnect Essentials          : 5000         perpetual
Other VPN Peers                 : 5000         perpetual
Total VPN Peers                 : 5000         perpetual
AnyConnect for Mobile          : Enabled       perpetual
AnyConnect for Cisco VPN Phone : Enabled       perpetual
Advanced Endpoint Assessment    : Enabled       perpetual
Shared License                  : Disabled      perpetual
Total TLS Proxy Sessions       : 3000         perpetual
Botnet Traffic Filter           : Disabled      perpetual
```

```
IPS Module           : Disabled      perpetual
Cluster             : Enabled       perpetual
Cluster Members     : 2              perpetual
```

This platform has an ASA5555 VPN Premium license.

## ライセンス リソース割り当ての表示

リソース割り当てを表示するには、次のコマンドを使用します。

```
asa2(config)# sh resource allocation
Resource      Total    % of Avail
Conns[rate]   100(U)   0.00%
Inspects[rate] unlimited
Syslogs[rate] unlimited
Conns         unlimited
Hosts        unlimited
IPsec        unlimited
Mac-addresses unlimited
ASDM         10       5.00%
SSH         10       10.00%
Telnet      10       10.0%
Xlates     unlimited
AnyConnect  1000    10%
AnyConnectBurst 200    2%
OtherVPN   2000    20%
OtherVPNBurst 1000    10%
```

## ライセンス リソース使用率の表示

リソース使用率を表示するには、次のコマンドを使用します。



(注) **sh resource usage system controller all 0** コマンドを使用して、プラットフォーム制限として制限があるシステム レベルの使用率を表示することもできます。

```
ASA(config-ca-trustpoint)# sh resource usage
Resource      Current  Peak  Limit  Denied  Context
Conns         1        16   280000  0       System
Hosts         2        10   N/A    0       System
AnyConnect    2        25   1000   0       cust1
AnyConnectBurst 0        0    200   0       cust1
OtherVPN      1        1    2000   0       cust2
OtherVPNBurst 0        0    1000   0       cust2
```

## VPN セッションの制限

AnyConnect VPN セッション (IPsec/IKEv2 または SSL) を ASA で許可されているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-anyconnect-premium-or-essentials-limit** コマンドを使用します。セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。

ASA のライセンスで 500 の SSL VPN セッションが許可されていて、AnyConnect VPN セッション数を 250 に制限する場合は、次のコマンドを入力します。

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。

```
hostname(config)# no vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

## ID 証明書のネゴシエート時の使用

IKEv2 トンネルを AnyConnect クライアントとネゴシエートする場合、ASA は ID 証明書を使用する必要があります。ikev2 リモートアクセストラストポイントコンフィギュレーションの場合、次のコマンドを使用します。

```
crypto ikev2 remote-access trustpoint <name> [line<number>]
```

このコマンドを使用すると、AnyConnect クライアントは、エンドユーザのグループ選択をサポートできます。2 つのトラストポイントを同時に設定できます。RSA を 2 つ、ECDSA を 2 つ、またはそれぞれ 1 つずつ設定できます。ASA は、設定したトラストポイントリストをスキャンし、クライアントがサポートする最初の 1 つを選択します。ECDSA を使用する場合は、RSA トラストポイントの前に、このトラストポイントを設定する必要があります。

行番号オプションは、トラストポイントを挿入する行番号の場所を指定します。通常、このオプションは、別の行を削除および再追加しないで一番上にトラストポイントを挿入するために使用されます。行が指定されていない場合、ASA はリストの末尾にトラストポイントを追加します。

すでに存在するトラストポイントを追加しようとする、エラーが表示されます。削除するトラストポイント名を指定しないで `no crypto ikev2 remote-access trustpoint` コマンドを使用すると、すべてのトラストポイント コンフィギュレーションが削除されます。

## 暗号化コアのプールの設定

対称型マルチプロセッシング (SMP) プラットフォームでの暗号化コアの割り当てを変更して、AnyConnect TLS/DTLS トラフィックのスループットを向上させることができます。この変更によって、SSL VPN データパスが高速化され、AnyConnect、スマートトンネル、およびポート転送において、ユーザが認識できるパフォーマンス向上が実現します。次の手順では、シングルコンテキストモードまたはマルチコンテキストモードで暗号化コアのプールを設定します。

暗号化コア再分散が利用できるのは、次のプラットフォームです。

- 5585-X
- 5545-X

- 5555-X
- ASASM

## 手順

暗号アクセラレータ プロセッサの割り当てを指定します。

### crypto engine accelerator-bias

- [balanced] : 暗号化ハードウェア リソースを均等に分散します (Admin/SSL および IPsec コア)。
- [ipsec] : IPsec を優先するように暗号化ハードウェア リソースを割り当てます (SRTP 暗号化音声トラフィックを含む)。
- [ssl] : Admin/SSL を優先するように暗号化ハードウェア リソースを割り当てます。

例 :

```
hostname(config)# crypto engine ?
configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors

hostname(config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl - Allocate crypto hardware resources to favor SSL

hostname(config)# crypto engine accelerator-bias ssl
```

## ダイナミック スプリット トンネリングの設定

ダイナミック スプリット トンネリングでは、トンネルの確立後に、DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。ダイナミック スプリット トンネリングを設定するには、カスタム属性を作成し、グループ ポリシーに追加します。

### 始める前に

この機能を使用するには、AnyConnect リリース 4.5 (またはそれ以降) が必要です。詳細については、「[About Dynamic Split Tunneling](#)」を参照してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	次のコマンドで、WebVPN コンテキストにおけるカスタム属性タイプを定義します。 <pre>anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains</pre>	
ステップ 2	VPN トンネル外部のクライアントによるアクセスが必要な各クラウド/Web サービスについて、属性名を定義します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。属性値は VPN トンネルから除外するドメイン名のリストを含み、次の例のように、カンマ区切り値 (CSV) 形式にする必要があります。 <pre>anyconnect-custom-data dynamic-split-exclude-domains webex.com, webexconnect.com, tags.tiqcdn.com</pre>	
ステップ 3	次のコマンドで、以前に定義されているカスタム属性を特定のポリシーグループに追加します。これは、group-policy 属性のコンテキストで実行されます。 <pre>anyconnect-custom dynamic-split-exclude-domains value webex_service_domains</pre>	

## 次のタスク

スプリットを含むトンネリングが設定されている場合、ダイナミック スプリット除外は、スプリットを含むネットワークに DNS 応答 IP アドレスが 1 つ以上含まれる場合のみ、実行されません。DNS 応答 IP アドレスとスプリットを含むネットワークのいずれかの間にまったく重ならない場合、すべての DNS 応答 IP アドレスに一致するトラフィックはすでにトンネリングから除外されているため、ダイナミック スプリット除外の実行は不要です。

## アクティブな VPN セッションの表示

次のトピックでは、VPN セッション情報を表示する方法について説明します。

## IP アドレス タイプ別のアクティブな AnyConnect セッションの表示

コマンドラインインターフェイスを使用して、アクティブな AnyConnect セッションを表示するには、特権 EXEC モードで **show vpn-sessiondb anyconnect filter p-ipversion** または **show vpn-sessiondb anyconnect filter a-ipversion** コマンドを入力します。

- エンドポイントのパブリック IPv4 または IPv6 アドレスでフィルタリングされたアクティブな AnyConnect セッションを表示します。パブリックアドレスは、企業によってエンドポイントに割り当てられたアドレスです。

```
show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}
```

- エンドポイントの割り当てられた IPv4 または IPv6 アドレスでフィルタリングされたアクティブな AnyConnect セッションを表示します。割り当て済みアドレスは、ASA によって AnyConnect Secure Mobility Client に割り当てられたアドレスです。

```
show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}
```

### show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6] コマンドの出力例

```
hostname(config)# show vpn-sessiondb anyconnect filter p-ipversion v4

Session Type: AnyConnect

Username       : user1                Index           : 40
Assigned IP    : 192.168.17.10         Public IP       : 198.51.100.1
Protocol       : AnyConnect-Parent SSL-Tunnel
License        : AnyConnect Premium
Encryption     : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing        : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx       : 10570                Bytes Rx        : 8085
Group Policy   : GroupPolicy_SSLACCLIENT
Tunnel Group   : SSLACCLIENT
Login Time     : 15:17:12 UTC Mon Oct 22 2012
Duration       : 0h:00m:09s
Inactivity     : 0h:00m:00s
NAC Result     : Unknown
VLAN Mapping   : N/A                    VLAN            : none
```

### show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6] コマンドの出力

```
hostname(config)# show vpn-sessiondb anyconnect filter a-ipversion v6

Session Type: AnyConnect

Username       : user1                Index           : 45
Assigned IP    : 192.168.17.10
Public IP      : 2001:DB8:8:1:90eb:3fe5:9eea:fb29
Assigned IPv6  : 2001:DB8:9:1::24
Protocol       : AnyConnect-Parent SSL-Tunnel
License        : AnyConnect Premium
Encryption     : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing        : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
```

```

Bytes Tx      : 10662                Bytes Rx      : 17248
Group Policy  : GroupPolicy_SSL_IPv6  Tunnel Group  : SSL_IPv6
Login Time    : 17:42:42 UTC Mon Oct 22 2012
Duration      : 0h:00m:33s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                VLAN          : none

```

## IP アドレス タイプ別のアクティブなクライアントレス SSL VPN セッションの表示

コマンドライン インターフェイスを使用して、アクティブなクライアントレス SSL VPN セッションを表示するには、特権 EXEC モードで **show vpn-sessiondb webvpn filter ipversion** コマンドを入力します。

パブリック アドレスは、企業によってエンドポイントに割り当てられたアドレスです。

```
show vpn-sessiondb webvpn filter ipversion {v4 | v6}
```

### 例

```

hostname# sh vpn-sessiondb webvpn filter ipversion v4

Session Type: WebVPN

Username      : user1                Index        : 63
Public IP     : 171.16.17.6
Protocol      : Clientless
License       : AnyConnect Premium
Encryption    : Clientless: (1)RC4    Hashing       : Clientless: (1)SHA1
Bytes Tx      : 62454                Bytes Rx     : 13082
Group Policy  : SSLv6                Tunnel Group  : SSL_IPv6
Login Time    : 18:07:48 UTC Mon Oct 22 2012
Duration      : 0h:00m:16s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                VLAN         : none

```

## IP アドレス タイプ別のアクティブな LAN-to-LAN VPN セッションの表示

コマンドライン インターフェイスを使用して、アクティブなクライアントレス SSL VPN セッションを表示するには、特権 EXEC モードで **show vpn-sessiondb l2l filter ipversion** コマンドを入力します。

このコマンドは、接続のパブリック IPv4 アドレスまたはパブリック IPv6 アドレスでフィルタリングされたアクティブな LAN-to-LAN VPN セッションを表示します。

パブリック アドレスは、企業によってエンドポイントに割り当てられたアドレスです。

```
show vpn-sessiondb l2l filter ipversion {v4 | v6}
```

## ISE ポリシー適用について

Cisco Identity Services Engine (ISE) は、セキュリティポリシー管理および制御プラットフォームです。有線、ワイヤレス、VPN 接続のアクセス制御とセキュリティコンプライアンスを自動化し、シンプルにします。Cisco ISE は主に、Cisco TrustSec と連携してセキュアアクセスとゲストアクセスを提供し、個人所有デバイス持ち込み (BYOD) イニシアティブをサポートし、使用ポリシーを適用するために使用されます。

ISE Change of Authorization (CoA) 機能は、認証、認可、およびアカウントリング (AAA) セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザグループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インラインポスチャ実施ポイント (IPEP) は、ASA によって確立された各 VPN セッションにアクセスコントロールリスト (ACL) を適用する必要はありません。

ISE ポリシーの実施は、次の VPN クライアントでサポートされています。

- IPSec
- AnyConnect
- L2TP/IPSec



(注) ダイナミック ACL (dACL) やセキュリティグループタグ (SGT) などの一部のポリシー要素はサポートされていますが、VLAN 割り当てや IP アドレス割り当てなどのポリシー要素はサポートされていません。

システムフローは次のとおりです。

1. エンドユーザが VPN 接続を要求します。
2. ASA は、ISE に対してユーザを認証し、ネットワークへの限定アクセスを提供するユーザ ACL を受け取ります。
3. アカウントリング開始メッセージが ISE に送信され、セッションが登録されます。
4. ポスチャアセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。
5. ISE が CoA の「ポリシープッシュ」を介して ASA にポリシーの更新を送信します。これにより、ネットワークアクセス権限を高める新しいユーザ ACL が識別されます。





- (注) 後続の CoA 更新を介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

## ISE ポリシー適用に関する RADIUS サーバグループの設定

ISE ポリシーの評価と適用をイネーブルにするには、ISE サーバの RADIUS AAA サーバグループを設定し、サーバをグループに追加します。VPN にトンネルグループを設定する場合は、グループで AAA サービスにこのサーバグループを指定します。

### 手順

- ステップ 1** RADIUS AAA サーバグループを作成します。

#### **aaa-server group\_name protocol radius**

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)#
```

- ステップ 2** AAA サーバグループの RADIUS 動的認可 (CoA) サービスをイネーブルにします。

#### **dynamic-authorization [port number]**

ポートの指定は任意です。デフォルトは 1700 です。指定できる範囲は 1024 ~ 65535 です。

VPN トンネルでサーバグループを使用すると、対応する RADIUS サーバグループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。

```
hostname(config-aaa-server-group)# dynamic-authorization
```

- ステップ 3** 認証に ISE を使用しない場合は、RADIUS サーバグループに対し認可専用モードを有効にします。

#### **authorize-only**

これは、サーバグループを認可に使用するとき、RADIUS アクセス要求メッセージが、AAA サーバ用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。**radius-common-pw** コマンドを使用して RADIUS サーバの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバグループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウントिंगにこのサーバグループを使用する可能性があるからです。

```
hostname(config-aaa-server-group)# authorize-only
```

**ステップ 4** RADIUS 中間アカウントングアップデートメッセージの定期的な生成をイネーブルにします。

**interim-accounting-update [periodic [hours]]**

ISE は、ASA などの NAS デバイスから受信するアカウントングレコードに基づいて、アクティブセッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウントングメッセージまたはポスチャトランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブセッションについて ISE に定期的に中間アカウントング更新メッセージを送信するように、グループを設定します。

- **periodic[hours]** は、対象のサーバグループにアカウントングレコードを送信するように設定されたすべての VPN セッションのアカウントングレコードの定期的な生成と伝送をイネーブルにします。オプションで、これらの更新の送信間隔（時間単位）を含めることができます。デフォルトは 24 時間で、指定できる範囲は 1 ~ 120 時間です。
- （パラメータなし）。**periodic** キーワードなしでこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときのみ中間アカウントング更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウントングアップデートが生成されます。

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

**ステップ 5** （任意）ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL を結合します。

**merge-dacl {before-avpair | after-avpair}**

このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。

**before-avpair** オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの前に配置されるように指定します。

**after-avpair** オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの後に配置されるように指定します。

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

**ステップ 6** （任意）次のサーバを試す前にグループ内の RADIUS サーバに送信する要求の最大数を指定します。

**max-failed-attempts number**

範囲は、1～5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定している場合で、グループ内のすべてのサーバが応答しないとき、グループは応答なしと見なされ、フォールバック方式が試行されます。サーバグループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとします。

```
hostname(config-aaa-server-group)# max-failed-attempts 2
```

**ステップ 7** （任意）グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

**reactivation-mode {depletion [deadtime minutes] | timed}**

それぞれの説明は次のとおりです。

- **depletion [deadtime minutes]** は、グループ内のすべてのサーバが非アクティブになった後でのみ、障害が発生したサーバを再アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0～1440 分の範囲で指定できます。デフォルトは 10 分です。
- **timed** 30 秒のダウン時間の後、障害が発生したサーバを再アクティブ化します。

```
hostname(config-aaa-server-group)# reactivation-mode deadtime 20
```

**ステップ 8** （任意）グループ内のすべてのサーバにアカウントティングメッセージを送信します。

**accounting-mode simultaneous**

アクティブサーバだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

**ステップ 9** グループに ISE RADIUS サーバを追加します。

**aaa-server group\_name [(interface\_name)] host {server\_ip | name} [key]**

それぞれの説明は次のとおりです。

- **group\_name** は、RADIUS サーバグループの名前です。

- `(interface_name)` は、サーバが到達するために使用するインターフェイスの名前です。デフォルトは `(inside)` です。カッコは必須です。
- `host{server_ip | name}` は、ISE RADIUS サーバの IP アドレスまたはホスト名です。
- `key` は、接続を暗号化するためのオプションキーです。aaa-server-host モードに入った後で `key` コマンドを使用することで、このキーをより簡単に入力できます。キーを設定しないと、接続は暗号化されません（プレーンテキスト）。このキーは127文字までの英数字から構成され、大文字と小文字の区別があり、RADIUS サーバ上のキーと同じ値になります。

グループには複数のサーバを追加できます。

```
hostname(config)# aaa-server servergroup1 (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

## ISE ポリシーの適用の設定例

### パスワードによる ISE ダイナミック認証のための VPN トンネルの設定

次の例は、ISE サーバグループに、動的認可 (CoA) のアップデートと時間ごとの定期的なアカウントリングを設定する方法を示しています。ISE によるパスワード認証を設定するトンネルグループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

### ISE 認証のみの VPN トンネルの設定

次に、ISE でローカル証明書の検証と認可用のトンネルグループを設定する例を示します。サーバグループは認証用に使用されないため、`authorize-only` コマンドをサーバグループコンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

```
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

## ポリシーの適用のトラブルシューティング

次のコマンドは、デバッグに使用できます。

CoA のアクティビティを追跡するには：

```
debug radius dynamic-authorization
```

リダイレクト URL 機能を追跡するには：

```
debug aaa url-redirect
```

URL リダイレクト機能に対応する NP 分類ルールを表示するには：

```
show asp table classify domain url-redirect
```

## SSL の詳細設定

ASA は、Secure Sockets Layer (SSL) プロトコルと Transport Layer Security (TLS) を使用して、ASDM、クライアントレス SSLVPN、VPN、およびブラウザベースの各セッションのセキュアなメッセージ伝送を実現します。ASA が SSL ベースの VPN 接続と管理接続でサポートしているプロトコルは、SSLv3、TLSv1、TLSv1.1、および TLSv1.2 です。また、DTLS は AnyConnect VPN クライアントの接続に使用されます。

説明したように、次の暗号方式がサポートされています。

暗号化方式	TLSv1.1 / DTLS V1	TLSV12
AES128-GCM-SHA256	いいえ	はい
AES128-SHA	はい	はい
AES128-SHA256	いいえ	はい
AES256-GCM-SHA384	いいえ	はい
AES256-SHA	はい	はい
AES256-SHA256	いいえ	はい

暗号化方式	TLSv1.1 / DTLS V1	TLSv1.2
DERS-CBC-SHA	いいえ	いいえ
DES-CBC-SHA	はい	はい
DHE-RSA-AES128-GCM-SHA256	いいえ	はい
DHE-RSA-AES128-SHA	はい	はい
DHE-RSA-AES128-SHA256	いいえ	はい
DHE-RSA-AES256-GCM-SHA384	no	1
DHE-RSA-AES256-SHA	はい	はい
ECDHE-ECDSA-AES128-GCM-SHA256	いいえ	はい
ECDHE-ECDSA-AES128-SHA256	いいえ	はい
ECDHE-ECDSA-AES256-GCM-SHA384	いいえ	はい
ECDHE-ECDSA-AES256-SHA384	いいえ	はい
ECDHE-RSA-AES128-GCM-SHA256	はい	はい
ECDHE-RSA-AES128-SHA256	いいえ	はい
ECDHE-RSA-AES256-GCM-SHA384	いいえ	はい
ECDHE-RSA-AES256-SHA384	いいえ	はい
NULL-SHA	いいえ	いいえ
RC4-MD5	いいえ	いいえ
RC4-SHA	いいえ	いいえ



(注) リリース 9.4 (1) では、SSLv3 キーワードはすべて ASA 設定から削除されており、SSLv3 のサポートが ASA から削除されました。SSLv3 がイネーブルになっている場合は、SSLv3 オプションを指定したコマンドからブート時エラーが表示されます。ASA はデフォルトの TLSv1 に戻ります。

Citrix モバイルレシーバは TLS 1.1/1.2 プロトコルをサポートしていない可能性があります。互換性については、[https://www.citrix.com/content/dam/citrix/en\\_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf](https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf) を参照してください。

ASA が SSL/TLS 接続をネゴシエートする最小プロトコルバージョンを指定するには、次の手順を実行します。

## 手順

**ステップ 1** ASA が接続をネゴシエートする最小プロトコルバージョンを設定します。

```
ssl server-version [tlsv1 | tlsv1.1 | tlsv1.2 ]
```

それぞれの説明は次のとおりです。

- **tlsv1** : SSLv2 クライアントの hello を受け入れ、TLSv1 (以降) をネゴシエートするには、このキーワードを入力します。
- **tlsv1.1** : SSLv2 クライアントの hello を受け入れ、TLSv1.1 (以降) をネゴシエートするには、このキーワードを入力します。
- **tlsv1.2** : SSLv2 クライアントの hello を受け入れ、TLSv1.2 (以降) をネゴシエートするには、このキーワードを入力します。

例 :

例 :

```
hostname(config)# ssl server-version tlsv1.1
```

**ステップ 2** ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。

```
ssl client-version [tlsv1 | tlsv1.1 | tlsv1.2]
```

```
hostname(config)# ssl client-version tlsv1
```

tlsv1 キーワードを指定すると、ASA は TLSv1 クライアントの hello を送信し、TLSv1 以上をネゴシエートします。tlsv1.1 キーワードを指定すると、ASA は TLSv1.1 クライアントの hello を送信し、TLSv1.1 以上をネゴシエートします。tlsv1.2 キーワードを指定すると、ASA は TLSv1.2 クライアントの hello を送信し、TLSv1.2 以上をネゴシエートします。(SSL クライアントロールに対して DTLS は使用不可)

**ステップ 3** SSL、DTLS、および TLS プロトコルの暗号化アルゴリズムを指定します。

```
ssl cipher version [ level | custom string
```

それぞれの説明は次のとおりです。

- **version** 引数は、SSL、DTLS、または TLS プロトコルバージョンを指定します。サポートされているバージョンは次のとおりです。
  - **default** : 発信接続用の暗号セット。
  - **dtlsv1** : DTLSv1 着信接続用の暗号。

- dtls1.2 : DTLSv1.2 着信接続用の暗号。
  - tls1 : TLSv1 着信接続用の暗号。
  - tls1.1 : TLSv1.1 着信接続用の暗号。
  - tls1.2 : TLSv1.2 着信接続用の暗号。
- *level* 引数は、暗号強度を指定し、設定されている暗号の最低レベルを示します。次に、強度の有効な値を強度の低い順に示します。
    - all : NULL-SHA を含むすべての暗号が含まれます。
    - low : NULL-SHA を除くすべての暗号が含まれます。
    - medium (これはすべてのプロトコルバージョンのデフォルト値です) : NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除くすべての暗号が含まれます。
    - fips : NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く FIPS 準拠のすべての暗号が含まれます。
    - high (TLSv1.2 にのみ適用) : SHA-2 暗号を使用する AES-256 のみが含まれます。
  - *custom string* オプションを指定すると、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。詳細については、<https://www.openssl.org/docs/apps/ciphers.html> を参照してください。

推奨設定は [medium] です。[high] を使用すると、接続が制限されることがあります。custom を使用すると、少数の暗号のみが設定されている場合は、機能が制限されることがあります。デフォルトのカスタム値を制限すると、クラスタリングを含めて発信接続が制限されることがあります。

ASA によってサポートされる暗号の優先順位は次のとおりです。詳細については、コマンドリファレンスを参照してください。

このコマンドは、バージョン 9.3(2) から廃止された `ssl encryption` コマンドに代わるものです。

**ステップ 4** 1つのインターフェイスで複数のトラストポイントを可能にします。

**ssl trust-point name** [[**interface** *vpn1b-ip*] | **domain** *domain-name*]

```
hostname(config)# ssl trust-point www-cert domain www.example.com
```

**name** 引数は、トラストポイントの名前を指定します。**interface** 引数は、トラストポイントが設定されているインターフェイスの名前を指定します。**vpn1b-ip** キーワードは、インターフェイスにのみ適用され、このトラストポイントをこのインターフェイス上の VPN ロードバランシング クラスターの IP アドレスに関連付けます。**domain***domain-name* キーワードと引数のペアは、インターフェイスへのアクセスに使用される特定のドメイン名に関連付けられたトラストポイントを指定します。

インターフェイスあたり最大 16 個のトラストポイントを設定できます。



インターフェイスまたはドメインを指定しない場合は、トラストポイントが設定されていないすべてのインターフェイス用のフォールバック トラストポイントが作成されます。

**ssl trustpoint ?** コマンドを入力すると、使用可能な設定済みのトラストポイントが表示されません。**ssl trust-point name ?** コマンド（たとえば、**ssl trust-point mysslcert ?**）を入力した場合、trustpoint-SSL 証明書アソシエーションに使用可能な設定済みのインターフェイスが表示されません。

このコマンドを使用するときは、次のガイドラインに従ってください。

- **trustpoint** の値は、**crypto ca trustpoint name** コマンドで設定された CA トラストポイントの **name** である必要があります。
- **interface** の値は、あらかじめ設定されたインターフェイスの **nameif** 名である必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照する **ssl trust-point** エントリも削除されます。
- **ssl trust-point** エントリは、インターフェイスごとに 1 つと、インターフェイスを指定しないもの 1 つを保持できます。
- 同じトラストポイントを複数のエントリで再利用できます。
- **domain** キーワードで設定したトラストポイントは、複数のインターフェイスに適用されることがあります（接続方法によって異なります）。
- **domain-name** の値ごとに 1 つの **ssl trust-point** のみを保持できます。
- このコマンドを入力すると、次のエラーが表示される場合があります。

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values mismatch@x509_cmp.c:339
```

これは、ユーザが新しい証明書を設定して、以前に設定された証明書と置き換えたことを示しています。特に対処の必要はありません。

- 証明書は次の順序で選択されます。
  - 接続が **domain** キーワードの値に一致した場合、その証明書が最初に選択されます。（**ssl trust-point namedomain domain-name** コマンド）
  - ロードバランシングアドレスへの接続が確立された場合、**vpnlb-ip** 証明書が選択されます。（**ssl trust-point name interface vpnlb-ip** コマンド）
  - インターフェイスに対して設定された証明書。（**ssl trust-point name interface** コマンド）
  - インターフェイスに関連付けられていないデフォルトの証明書。（**ssl trust-point name**）
  - ASA の自己署名付き自己生成証明書。

**ステップ 5** TLS の DHE-RSA 暗号方式で使用される DH グループを指定します。

```
ssl dh-group [group1 | group2 | group5 | group14 | group24]
hostname(config)# ssl dh-group group5
```

グループ 1 および 2 は、Java 7 およびそれ以前のバージョンと互換性があります。グループ 5、14、および 24 は、Java 7 と互換性がありません。すべてのグループが Java 8 と互換性があります。グループ 14 と 24 は FIPS 準拠です。デフォルト値は `ssl dh-group group2` です。

**ステップ 6** TLS の ECDHE-ECDSA 暗号方式で使用されるグループを指定します。

```
ssl ecdh-group [group19 | group20 | group21]
hostname(config)# ssl ecdh-group group20
```

`group19` キーワードは、グループ 19 (256 ビット EC) を設定します。`group20` キーワードは、グループ 20 (384 ビット EC) を設定します。`group21` キーワードは、グループ 21 (521 ビット EC) を設定します。

デフォルト値は `ssl ecdh-group group19` です。

(注) 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。

---

例

## 永続的 IPSec トンネル フロー

リリース 8.0.4 よりも前の ASA ソフトウェア バージョンを実行するネットワークでは、IPSec トンネルを通過する既存の IPsec LAN-to-LAN またはリモート アクセス TCP トラフィック フローは、トンネルがドロップするとドロップされます。これらのフローは、トンネルが元に戻ると、必要に応じて再作成されます。このポリシーは、リソース管理およびセキュリティの観点から有効です。ただし、このような動作がユーザ（特に PIX から ASA のみの環境に移行しているユーザ）およびレガシー TCP アプリケーション（容易に再起動しない、またはトンネルを頻繁にドロップするゲートウェイが含まれたネットワーク内にある）に問題を引き起こす場合があります（詳細については、CSCsj40681 および CSCsi47630 を参照してください）。

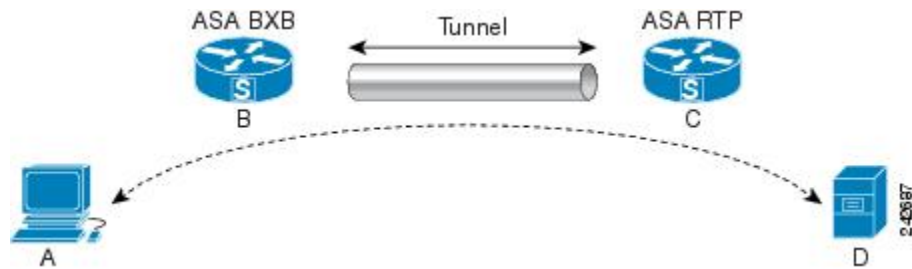
永続的な IPsec トンネルフロー機能で、この問題に対処します。この機能をイネーブルにすると、ASA はステートフル (TCP) トンネルフローを維持して再開します。他のすべてのフローは、トンネルがドロップしたときにドロップされ、新しいトンネルが設定されたときに再確立する必要があります。



(注) この機能は、ネットワーク拡張モードで実行されている IPsec LAN-to-LAN トンネルおよび IPsec リモートアクセス トンネルをサポートします。IPsec または AnyConnect/SSL VPN リモートアクセス トンネルはサポートしていません。

次に、永続的 IPsec トンネル フロー機能がどのように動作するか例を示します。

図 2: ネットワーク シナリオ



この例では、BXB および RTP ネットワークが 1 対のセキュリティ アプライアンスによりセキュア LAN-to-LAN トンネルを介して接続しています。BXB ネットワークの PC は RTP ネットワークのサーバからセキュア トンネルを介して FTP 転送を実行しています。このシナリオでは、PC がサーバにログインし、転送を開始した後でトンネルが何らかの理由でドロップしたと想定しています。この時点でもデータは流れようとしているため、トンネルは再確立されていますが、FTP 転送が完了しません。ユーザは、サーバにログインして転送を終了させ、もう一度やり直す必要があります。ただし、永続的 IPsec トンネル フローがイネーブルになっている場合、タイムアウト間隔以内にトンネルが再作成される限り、セキュリティ アプライアンスはこのフローの履歴 (状態情報) を維持するため、データは新しいトンネルを通じて正常に流れ続けます。

### シナリオ

次の項では、ドロップ後に復旧されたトンネルのデータフローの状態を、永続的 IPsec トンネルフロー機能がディセーブルになっている場合と、この機能がイネーブルになっている場合の順に説明します。どちらの場合も、ネットワークのイラストについては前の図を参照してください。この図の場合：

- フロー B-C は、トンネルを定義し、暗号化された ESP データを送送します。
- フロー A-D は、FTP 転送の TCP 接続で、フロー B-C で定義されたトンネルを通過します。このフローには、ファイアウォールで TCP/FTP フローを検査するとき使用される状態情報も含まれています。状態情報は重要であり、転送が進行するとファイアウォールによって継続的にアップデートされます。



(注) 各方向の逆フローは簡略化のため省略されています。

### ディセーブル化された永続的な IPsec トンネル フロー

LAN-2-LAN トンネルがドロップすると、A-D フローと B-C フローの両方と、それらに属するすべての状態情報が削除されます。その後、トンネルが再確立され、フロー B-C が再作成され、トンネリングされたデータの伝送を再開できるようになります。ただし、TCP/FTP フロー A-D に問題が発生します。この時点までの FTP 転送のフローを説明する状態情報が削除されているため、ステートフルファイアウォールは、インフライト FTP データをブロックし、A-D フローの作成を拒否します。今まで存在していたこのフロー履歴が失われると、ファイアウォールは FTP 転送を迷子の TCP パケットとして処理し、ドロップします。これはデフォルトの動作です。

### イネーブル化された永続的な IPsec トンネル フロー

永続的 IPsec トンネル フロー機能がイネーブルの場合、タイムアウト時間内にトンネルが再作成される限り、ASA は A-D フローの状態情報にアクセスできるため、データは正常に流れ続けます。

この機能がイネーブルの場合、ASA はフローを個別に処理します。つまり、B-C フローによって定義されたトンネルがドロップされても、A-D フローは削除されません。ASA はステートフル (TCP) トンネルフローを維持し、再開します。他のフローはすべてドロップされ、新しいトンネルで再確立される必要があります。これは、トンネルフローのセキュリティポリシーを弱めることはありません。ASA はトンネルがダウンしているときに A-D フローに到着するパケットをドロップするからです。

トンネル TCP フローはドロップされないため、クリーンアップは TCP タイムアウトに依存します。ただし、特定のトンネルフローのタイムアウトがディセーブルになっている場合、手動または他の方法 (ピアからの TCP RST など) によってクリアされるまで、そのフローはシステム内で保持されます。

## CLI を使用した永続的 IPsec トンネル フローの設定

設定例

### 永続的な IPsec トンネル フローのトラブルシューティング

`show asp table` コマンドと `show conn` コマンドは両方とも、永続的 IPsec トンネル フローの問題のトラブルシューティングに役立ちます。

### 永続的 IPsec トンネル フロー機能はイネーブルになっていますか？

特定のトンネルでこの機能がイネーブルになっているかを確認するには、`show asp table` コマンドを使用してトンネルに関連付けられた VPN コンテキストを調べます。`show asp table vpn-context` コマンドは、次の例に示すように (読みやすくするために太字を追加)、トンネルがドロップした後にステートフルフローを維持する各コンテキストに「+PRESERVE」フラグを表示します。

```
hostname(config)# show asp table vpn-context
```

```
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=000000000, rk=000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=000000000, rk=000000000,
gc=0
```

```
-----
hostname(config)# show asp table vpn-context detail
```

```
VPN CTX = 0x0005FF54
```

```
Peer IP = ASA_Private
Pointer = 0x6DE62DA0
State = UP
Flags = DECR+ESP+PRESERVE
SA = 0x001659BF
SPI = 0xB326496C
Group = 0
Pkts = 0
Bad Pkts = 0
Bad SPI = 0
Spoof = 0
Bad Crypto = 0
Rekey Pkt = 0
Rekey Call = 0
```

```
VPN CTX = 0x0005B234
```

```
Peer IP = ASA_Private
Pointer = 0x6DE635E0
State = UP
Flags = ENCR+ESP+PRESERVE
SA = 0x0017988D
SPI = 0x9AA50F43
Group = 0
Pkts = 0
Bad Pkts = 0
Bad SPI = 0
Spoof = 0
Bad Crypto = 0
Rekey Pkt = 0
Rekey Call = 0
```

```
hostname(config)#
```

```
Configuration and Restrictions
```

```
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

## 孤立したフローの検索

LAN-to-LANまたはネットワーク拡張モードトンネルがドロップし、タイムアウト前に復旧しなかった場合、孤立したトンネルフローが数多く発生することがあります。このようなフローはトンネルのダウンによって切断されませんが、これらのフローを介して通過を試みるすべてのデータがドロップされます。これらのフローを確認するには、**show conn** コマンドを次の例に示すように使用します（強調するため、およびユーザ入力を示すために太字を追加）。

```
asa2(config)# show conn detail
```

```
9 in use, 14 most used
```

```
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
E - outside back connection, F - outside FIN, f - inside FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
```

```

i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
k - Skinny media, M - SMTP data, m - SIP media, n - GUP
O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
q - SQL*Net data, R - outside acknowledged FIN,
R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
V - VPN orphan, W - WAAS,
X - inspected by service module

```

次の例に、**show conn** コマンドの出力例を示します。**V** フラグで示されているとおり、孤立したフローが存在します。

```

hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00 bytes 1048 flags UOVb
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle bytes 1048 flags UIOb

```

孤立したフローがあるこのような接続へのレポートを制限するには、次の例で示すように、**show conn state** コマンドに **vpn\_orphan** オプションを追加します。

```

hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013 idle 0:00:00 bytes 2841019 flags
UOVb

```