CHAPTER 3

VPN の一般パラメータの設定

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。内容は次のとおりです。

（注） この章の SSL VPN は、クライアントレス（ブラウザベース）SSL VPN が指定されていない限り、SSL VPN クライアント（AnyConnect 2.x またはその前身である SVC 1.x）を指します。

単一のルーテッド モードでの VPN の設定

VPN は、単一のルーテッド モードでのみ動作します。セキュリティ コンテキストが含まれるコンフィギュレーション（マルチモード ファイアウォールとも呼ばれる）、またはアクティブ/アクティブ ステートフル フェールオーバーが含まれるコンフィギュレーションでは、VPN 機能は利用できません。

例外として、管理上の目的で、トランスペアレント モードでの ASA への接続（通過はしない）を 1 つ設定して使用することができます。

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るため、セキュリティが向上します。

構文は、**sysopt connection permit-vpn** です。このコマンドには、キーワードも引数もありません。

次の例では、ALC 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** が設定されている間は、外部インターフェイスで access-group が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が許可されます。これは、**deny ip any any** ACL を呼び出します。

外部インターフェイスのアクセス コントロール リスト（ACL）と共に **no sysopt permit-vpn** コマンドを使用して、サイトツーサイト VPN またはリモート アクセス VPN 経由での保護されたネットワークへのアクセスを制御しようとしても、うまくいきません。

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。つまり、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。

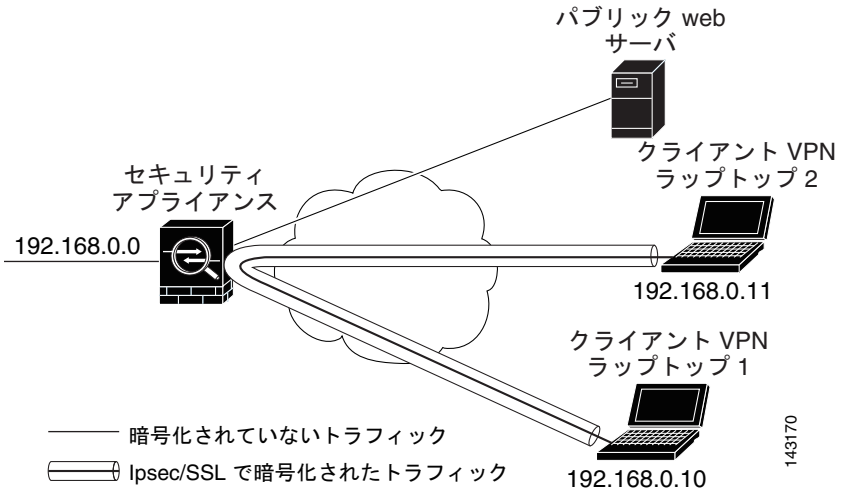
インターフェイス内トラフィックの許可（ヘアピニング）

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。

別のアプリケーションでは、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ちます。

図 3-1 では、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 3-1　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** 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を許可します。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 パラメータの設定に関する章を参照してください。

ヘアピニングを使用するには、次の項で説明するように、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 プールですでにパブリック 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 間ヘアピニングは、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 セッションの数を 1 から最大数まで指定します。

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 セッションの数を 1 から最大数まで指定します。これには、Cisco VPN Client（IPsec IKEv1）、LAN-to-LAN VPN、およびクライアントレス SSL 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と VPN 3002 ハードウェア クライアント イメージを、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。VPN 3002 ハードウェア クライアント ユーザの場合、アップデートは通知せずに自動的に行われます。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。

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更新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 タイプは、**win9X**（Windows 95、Windows 98、および Windows ME プラットフォーム）、**winnt**（Windows NT 4.0、Windows 2000、および Windows XP プラットフォーム）、**windows**（すべての Windows ベースのプラットフォーム）、および **vpn3002**（VPN 3002 ハードウェア クライアント）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。VPN 3002 ハードウェア クライアントの場合、代わりにプロトコル tftp:// を指定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 と更新を取得するための 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）。

VPN 3002 クライアントはユーザの介入なしで更新され、ユーザは通知メッセージを受信しません。次の例は、VPN 3002 ハードウェア クライアントだけに適用されます。トンネル グループ ipsec 属性コンフィギュレーション モードを開始すると、このコマンドによって、IPsec リモート アクセス トンネル グループ **salesgrp** 用のクライアント アップデート パラメータが設定されます。次の例では、リビジョン番号 4.7 を指定し、TFTP プロトコルを使用して、更新されたソフトウェアを IP アドレス 192.168.1.1 のサイトから取得します。

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
```

```
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
hostname(config-tunnel-ipsec)#
```

（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、次回ログイ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。VPN 3002 クライアントはユーザの介入なしで更新され、ユーザは通知メッセージを受信しません。

（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生じた場合は、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ことが必要になる場合があります。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。

制限事項

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 Cisco VPN Client（IKEv1）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。

手順の詳細

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。

```
prompt# 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 オブジェクトおよび show run nat reports レポートから非表示になります。

ロード バランシングの概要

同じネットワークに接続されている 2 つ以上の ASA または VPN コンセントレータを使用しているリモート アクセス コンフィギュレーションがある場合、それぞれのセッションの負荷を共有するようにこれらのデバイスを設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングを実装するには、同じプライベート LAN-to-LAN ネットワーク、プライベート サブネット、およびパブリック サブネット上の 2 つ以上のデバイスを論理的に*仮想クラスタ*にグループ化します。

セッションの負荷は、仮想クラスタ内のすべてのデバイスに分散されます。ロードバランシングにより、セッションのトラフィックはクラスタ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システム リソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

仮想クラスタ内の 1 つのデバイスである *仮想クラスタ マスター*は、着信トラフィックを*バックアップ デバイス*と呼ばれる他のデバイスに転送します。仮想クラスタ マスターは、クラスタ内のすべてのデバイスをモニタし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。仮想クラスタ マスターの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。たとえば、現在の仮想クラスタ マスターで障害が発生すると、クラスタ内のバックアップ デバイスの 1 つがその役割を引き継いで、すぐに新しい仮想クラスタ マスターになります。

仮想クラスタは、外部のクライアントには 1 つの*仮想クラスタ IP アドレス*として表示されます。この IP アドレスは、特定の物理デバイスに結び付けられていません。現在の仮想クラスタ マスターに属しているため、仮想のアドレスです。接続の確立を試みている VPN クライアントは、最初にこの仮想クラスタ IP アドレスに接続します。仮想クラスタ マスターは、クラスタ内で使用できるホストのうち、最も負荷の低いホストのパブリック IP アドレスをクライアントに返します。2 回めのトランザクション（ユーザに対しては透過的）になると、クライアントはホストに直接接続します。仮想クラスタ マスターは、このようにしてリソース全体に均等かつ効率的にトラフィックを転送します。

（注） Cisco VPN Client または Cisco 3002 ハードウェア クライアント以外のすべてのクライアントは、通常どおり ASA に直接接続する必要があります。これらのクライアントは、仮想クラスタ IP アドレスを使用しません。

クラスタ内のマシンで障害が発生すると、終了されたセッションはただちに仮想クラスタ IP アドレスに再接続できます。次に、仮想クラスタ マスターは、クラスタ内の別のアクティブ デバイスにこれらの接続を転送します。仮想クラスタ マスター自体に障害が発生した場合、クラスタ内のバックアップ

デバイスが、ただちに新しい仮想セッション マスターを自動的に引き継ぎます。クラスタ内の複数のデバイスで障害が発生しても、クラスタ内のデバイスが 1 つ稼働していて使用可能である限り、ユーザはクラスタに引き続き接続できます。

ロード バランシングとフェールオーバーの比較

ロード バランシングとフェールオーバーはどちらもハイ アベイラビリティ機能ですが、これらは機能も要件も異なります。場合によっては、ロード バランシングとフェールオーバーの両方を使用できます。次の項では、これらの機能の違いについて説明します。

ロード バランシング

ロード バランシングとは、リモートアクセス VPN トラフィックを、仮想クラスタ内のデバイス間で均等に分配するメカニズムのことです。この機能は、スループットまたはその他の要因を考慮しない単純なトラフィックの分散に基づいています。ロードバランシング クラスタは 2 つ以上のデバイスで構成され、そのうちの 1 つが仮想マスターとなり、それ以外のデバイスはバックアップとなります。これらのデバイスは、完全に同じタイプである必要はなく、同じソフトウェア バージョンやコンフィギュレーションを使用する必要もありません。

仮想クラスタ内のすべてのアクティブなデバイスがセッションの負荷を伝送します。ロードバランシングにより、トラフィックはクラスタ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システム リソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

フェールオーバー

フェールオーバー設定には、同じ ASA が 2 台、専用のフェールオーバー リンク（オプションで、ステートフル フェールオーバー リンク）で相互に接続されている必要があります。アクティブ インターフェイスおよび装置のヘルスがモニタされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。これらの条件に一致した場合は、フェールオーバーが行われます。フェールオーバーは、VPN とファイアウォールの両方のコンフィギュレーションをサポートします。

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバーをサポートします。VPN 接続は、アクティブ/スタンバイの単一ルーテッド モードでのみ実行されます。アクティブ/アクティブ フェールオーバーにはマルチコンテキスト モードが必要であるため、VPN 接続をサポートしません。

アクティブ/アクティブ フェールオーバーでは、両方の装置がネットワーク トラフィックを渡すことができます。これは、同じ結果になる可能性がありますが、真のロード バランシングではありません。フェールオーバーが行われると、残りのアクティブ装置が、設定されたパラメータに基づいて結合されたトラフィックの通過を引き継ぎます。したがって、アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにする必要があります。

アクティブ/スタンバイ フェールオーバーでは、1 つの装置だけがトラフィックを通過させることができ、もう 1 つの装置はスタンバイ状態で待機して、トラフィックを通過させません。アクティブ/スタンバイ フェールオーバーでは、2 番目の ASA を使用して、障害の発生した装置の機能を引き継ぎます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてスタンバイ装置がアクティブ状態に変わります。アクティブになる装置が、障害の発生した装置の IP アドレス（または、トランスペアレント ファイアウォールの場合は管理 IP アドレス）および MAC アドレスを引き継いで、トラフィックの転送を開始します。現在スタンバイになっている装置が、アクティブ装置のスタンバイの IP アドレスを引き継ぎます。アクティブ装置で障害が発生すると、スタンバイ装置は、クライアント VPN トンネルを中断することなく引き継ぎます。

ロード バランシングの実装

ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPsec 共有秘密情報を確立することによりロードバランシング クラスタを設定する。クラスタ内のすべてのデバイスに対してこれらの値を同一に設定します。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

（注）　VPN ロード バランシングには、アクティブな 3DES または AES ライセンスが必要です。ASA は、ロード バランシングをイネーブルにする前に、この暗号化ライセンスの存在をチェックします。アクティブな 3DES または AES ライセンスを検出できない場合、ASA は、ロード バランシングのイネーブル化を回避し、さらにライセンスがこの使用を許可していない限り、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回避します。

前提条件

ロード バランシングはデフォルトではディセーブルになっています。ロード バランシングは明示的にイネーブルにする必要があります。

まず、パブリック（外部）インターフェイスおよびプライベート（内部）インターフェイスを設定し、さらに仮想クラスタ IP アドレスが参照するインターフェイスを事前に設定しておく必要があります。これらのインターフェイスに異なる名前を設定するには、**interface** コマンドと **nameif** コマンドを使用します。この項では、これ以降の参照に外部および内部の名前を使用します。

クラスタに参加するすべてのデバイスは、同じクラスタ固有の値（IP アドレス、暗号化設定、暗号キー、およびポート）を共有する必要があります。

適格なプラットフォーム

ロードバランシング クラスタには、ASA モデルの ASA 5510（Plus ライセンスあり）および Model 5520 以降を含めることができます。クラスタには Cisco 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。

適格なクライアント

ロード バランシングは、次のクライアントで開始されるリモート セッションでのみ有効です。

- Cisco AnyConnect VPN Client（Release 2.0 以降）
- Cisco VPN Client（Release 3.0 以降）
- Cisco ASA 5505 ASA（Easy VPN クライアントとして動作している場合）
- Cisco VPN 3002 Hardware Client（Release 3.5 以降）
- Easy VPN クライアントとして動作している場合、Cisco PIX 501/506E
- IKE リダイレクトをサポートする Cisco IOS EZVPN クライアント デバイス（IOS 831/871）
- クライアントレス SSL VPN（クライアントではない）

ロード バランシングは、IPsec クライアント セッションと SSL VPN クライアントおよびクライアントレス セッションで機能します。LAN-to-LAN を含む他のすべての VPN 接続タイプ（L2TP、PPTP、L2TP/IPsec）は、ロード バランシングがイネーブルになっている ASA に接続できますが、これらの接続タイプはロード バランシングには参加できません。

VPN ロードバランシングのアルゴリズム

マスター デバイスには、バックアップ クラスタ メンバーを IP アドレスの昇順にソートしたリストが保持されます。各バックアップ クラスタ メンバーの負荷は、整数の割合（アクティブ セッション数）として計算されます。AnyConnect の非アクティブ セッションは、ロード バランシングの SSL VPN 負荷に数えられません。マスター デバイスは、IPsec トンネルと SSL VPN トンネルを負荷が最も低いデバイスに、その他のデバイスより負荷が 1% 高くなるまでリダイレクトします。すべてのバックアップ クラスタ メンバーの負荷がマスターより 1% 高くなると、マスター デバイスは自分自身に対してリダイレクトします。

たとえば、1 つのマスターと 2 つのバックアップ クラスタ メンバーがある場合に、次のサイクルが当てはまります。

（注） すべてのノードは 0% から始まり、すべての割合は四捨五入されます。

1. マスター デバイスは、すべてのメンバにマスターよりも 1% 高い負荷がある場合に、接続を使用します。
2. マスターが接続を使用しない場合、セッションは、最もロード率が低いバックアップ デバイスが処理します。
3. すべてのメンバに同じ割合の負荷がかかっている場合、セッション数が最も少ないバックアップ デバイスがセッションを取得します。
4. すべてのメンバに同じ割合の負荷と同じ数のセッションがある場合、IP アドレス数が最も少ないデバイスがセッションを取得します。

VPN ロードバランシング クラスタ コンフィギュレーション

ロードバランシング クラスタは、次の制限に従って、同じリリース、または混在リリースの ASA と、VPN 3000 コンセントレータ、あるいはこれらの組み合わせで構成できます。

- 同じリリースの ASA、またはすべて VPN 3000 コンセントレータで構成されるロードバランシング クラスタは、IPsec、AnyConnect、およびクライアントレス SSL VPN セッションの組み合わせに対してロードバランシングを実行できます。
- 同じリリースの ASA および VPN 3000 コンセントレータの両方で構成されるロードバランシング クラスタは、IPsec、AnyConnect、およびクライアントレス SSL VPN クライアントとクライアントレス セッションの組み合わせに対してロード バランシングを実行できます。
- 混在リリースの ASA または同じリリースの ASA および VPN 3000 コンセントレータあるいはこれら両方で構成されるロードバランシング クラスタは、IPsec セッションのみをサポートできます。ただし、このようなコンフィギュレーションでは、ASA は、それぞれの IPsec のキャパシティに完全に到達しない可能性があります。シナリオ 1：SSL VPN 接続のない混在クラスタは、この状況を示しています。

Release 7.1(1) 以降、IPsec セッションと SSL VPN セッションは、クラスタ内の各デバイスが伝送する負荷を決定するときに均等にカウントまたは重み付けします。これは、ASA Release 7.0(x) ソフトウェアと VPN 3000 コンセントレータのロードバランシング計算からの変更です。両方のプラットフォームで、一部のハードウェア プラットフォームが SSL VPN セッションの負荷を IPSec セッションの負荷とは異なる方法で計算する重み付けアルゴリズムが使用されます。

クラスタの仮想マスターは、クラスタのメンバにセッション要求を割り当てます。ASA は、すべてのセッション、SSL VPN または IPsec を同等と見なし、それらを同等に割り当てます。許可する IPsec セッションと SSL VPN セッションの数は、コンフィギュレーションおよびライセンスで許可されている最大数まで設定できます。これらの制限の設定方法については、VPN セッション制限の設定を参照してください。

ロードバランシング クラスタで最大 10 のノードはテスト済みです。これよりクラスタが多くても機能しますが、そのようなトポロジは正式にはサポートされていません。

一部の一般的な混在クラスタのシナリオ

混在コンフィギュレーション、つまりロードバランシング クラスタにさまざまな ASA ソフトウェア リリースを実行しているデバイスが含まれている、または ASA Release 7.1(1) 以降および VPN 3000 コンセントレータを実行している ASA が少なくとも 1 つ含まれる場合、最初のクラスタ マスターで障害が発生し、別のデバイスがマスターを引き継ぐときに、重み付けアルゴリズムの違いが問題になります。

次のシナリオは、ASA Release 7.1(1)、ASA Release 7.0(x) ソフトウェアを実行している ASA と VPN 3000 シリーズ コンセントレータの混在で構成されているクラスタでの VPN ロードバランシングの使用を示しています。

シナリオ 1：SSL VPN 接続のない混在クラスタ

このシナリオでは、クラスタは ASA と VPN 3000 コンセントレータの混在で構成されています。ASA クラスタ ピアには、ASA Release 7.0(x) を実行しているものも、Release 7.1(1) を実行しているものもあります。7.1(1) 以前のピアおよび VPN 3000 ピアには、SSL VPN 接続はなく、7.1(1) クラスタ ピアには、SSL VPN の基本ライセンスのみあり、2 つの SSL VPN セッションは許可されますが、SSL VPN 接続はありません。この場合、すべての接続は IPsec であり、ロード バランシングは良好に機能します。

2 つの SSL VPN ライセンスは、ユーザの最大 IPsec セッション制限の活用にはほとんど影響を及ぼしません。また、これは VPN 3000 コンセントレータがクラスタ マスターの場合に限られます。一般に、混在クラスタ内の ASA の SSL VPN ライセンスの数が少なければ少ないほど、IPsec セッションしかないシナリオで IPsec セッションの制限に達することができる ASA 7.1(1) デバイスへの影響も小さくなります。

シナリオ 2：SSL VPN 接続を処理する混在クラスタ

たとえば、ASA Release 7.1(1) ソフトウェアを実行している ASA が最初のクラスタ マスターで、そのデバイスに障害が発生したとします。クラスタ内の別のデバイスが自動的にマスターを引き継ぎ、そのクラスタ内のプロセッサの負荷を決定するためにそのデバイス独自のロードバランシング アルゴリズムを適用します。ASA Release 7.1(1) ソフトウェアを実行しているクラスタ マスターは、そのソフトウェアが提供する方法以外では、セッションの負荷を重み付けすることはできません。そのため、IPsec および SSL VPN セッションの負荷の組み合わせを、以前のバージョンを実行する ASA デバイスにも、VPN 3000 コンセントレータにも適切に割り当てることができません。これとは逆に、クラスタ マスターとして動作している VPN 3000 コンセントレータは、ASA Release 7.1(1) ASA に負荷を適切に割り当てることができません。次のシナリオは、このジレンマを示しています。

このシナリオは、クラスタが ASA と VPN 3000 コンセントレータの混在で構成されているという点において、前述のシナリオと似ています。ASA クラスタ ピアには ASA Release 7.0(x) を実行しているものも、Release 7.1(1) を実行しているものもあります。ただし、この場合は、クラスタは SSL VPN 接続だけでなく IPsec 接続も処理されます。

ASA Release 7.1(1) 以前のソフトウェアを実行しているデバイスがクラスタ マスターである場合、マスターは実質的に Release 7.1(1) 以前のプロトコルとロジックを適用します。つまり、セッションはそのセッション制限を超えているロードバランシング ピアに転送される場合もあります。その場合、ユーザはアクセスを拒否されます。

クラスタ マスターが ASA Release 7.0(x) ソフトウェアを実行しているデバイスである場合、古いセッション重み付けアルゴリズムは、クラスタ内の 7.1(1) 以前のピアにのみ適用されます。この場合、アクセスが拒否されることはありません。これは、7.1(1) 以前のピアは、セッション重み付けアルゴリズムを使用するため、負荷がより軽くなっています。

ただし、7.1(1) ピアが常にクラスタ マスターであることは保証できないため、問題が発生します。クラスタ マスターで障害が発生すると、別のピアがマスターの役割を引き継ぎます。新しいマスターは、適格なピアのいずれかになります。結果を予測することは不可能であるため、このタイプのクラスタを構成しないことを推奨します。

ロード バランシングの設定

ロードバランシングを使用するには、クラスタに参加する各デバイスに対して次の要素を設定します。

- パブリック インターフェイスとプライベート インターフェイス
- VPN ロードバランシング クラスタ属性

（注） クラスタに参加するすべてのデバイスには、クラスタ内でのデバイス プライオリティを除き、同一のクラスタ コンフィギュレーションを設定する必要があります。

（注） Active/Active ステートフル フェールオーバー、または VPN ロードバランシングを使用している場合、ローカル CA 機能はサポートされません。ローカル CA を別の CA の下位に置くことはできません。ローカル CA はルート CA にしかなれません。

ロード バランシング用のパブリック インターフェイスとプライベート インターフェイスの設定

ロードバランシング クラスタ デバイス用のパブリック（外部）インターフェイスとプライベート（内部）インターフェイスを設定するには、次の手順を実行します。

ステップ 1　vpn-load-balancing コンフィギュレーション モードで、**lbpublic** キーワードを指定して **interface** コマンドを入力し、ASA にパブリック インターフェイスを設定します。このコマンドは、このデバイスのロード バランシングのためのパブリック インターフェイスの名前または IP アドレスを指定します。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

ステップ 2　vpn-load-balancing コンフィギュレーション モードで、**lbprivate** キーワードを指定して **interface** コマンドを入力し、ASA にプライベート インターフェイスを設定します。このコマンドで、このデバイスのロード バランシングのためのプライベート インターフェイスの名前または IP アドレスを指定します。

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

ステップ 3　このデバイスを割り当てるためのクラスタ内でのプライオリティを設定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。プライオリティを高く設定すると（たとえば 10）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

```
hostname(config-load-balancing)# priority number
hostname(config-load-balancing)#
```

たとえば、このデバイスにクラスタ内でのプライオリティ 6 を割り当てるには、次のコマンドを入力します。

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

ステップ 4　このデバイスにネットワーク アドレス変換を適用する場合は、デバイスに割り当てられた NAT アドレスを指定して **nat** コマンドを入力します。IPv4 および IPv6 アドレスを定義するか、デバイスのホスト名を指定できます。

```
hostname(config-load-balancing)# nat ipv4_address ipv_address
hostname(config-load-balancing)#
```

たとえば、このデバイスに NAT アドレス 192.168.30.3 および 2001:DB8::1 を割り当てるには、次のコマンドを入力します。

```
hostname(config-load-balancing)# nat 192.168.30.3 2001:DB8::1
hostname(config-load-balancing)#
```

ロード バランシング クラスタ属性の設定

クラスタ内の各デバイスのロードバランシング クラスタ属性を設定するには、次の手順を実行します。

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 **vpn load-balancing** コマンドを入力して、VPN ロード バランシングをセットアップします。

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

これで vpn-load-balancing コンフィギュレーション モードに入るため、ここで残りのロードバランシング属性を設定できます。

ステップ 2　このデバイスが属しているクラスタの IP アドレスまたは完全修飾ドメイン名を設定します。このコマンドは、仮想クラスタ全体を表す単一の IP アドレスまたは FQDN を指定します。仮想クラスタ内のすべての ASA が共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。IPv4 アドレスまたは IPv6 アドレスを指定できます。

```
hostname(config-load-balancing)# cluster ip address ip_address
hostname(config-load-balancing)#
```

たとえば、クラスタ IP アドレスを IPv6 アドレス 2001:DB8::1 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster ip address 2001:DB8::1
hostname(config-load-balancing)#
```

ステップ 3　クラスタ ポートを設定します。次のコマンドは、このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロード バランシングに使用する UDP の宛先ポート番号を入力します。

```
hostname(config-load-balancing)# cluster port port_number
hostname(config-load-balancing)#
```

たとえば、クラスタ ポートを 4444 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster port 4444
hostname(config-load-balancing)#
```

ステップ 4　（任意）クラスタに対する IPsec 暗号化をイネーブルにします。デフォルトでは暗号化は使用されません。このコマンドは、IPsec 暗号化をイネーブルまたはディセーブルにします。このチェック属性を設定する場合は、まず共有秘密情報を指定して検証する必要があります。仮想クラスタ内の ASA は、IPsec を使用して LAN-to-LAN トンネル経由で通信します。デバイス間で通信されるすべてのロード バランシング情報が暗号化されるようにするには、この属性をイネーブルにします。

```
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

（注）　暗号化を使用する場合、事前にロードバランシング内部インターフェイスを設定しておく必要があります。そのインターフェイスがロードバランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

クラスタの暗号化を設定したときにロードバランシング Inside インターフェイスがイネーブルになっており、仮想クラスタ内の参加デバイスを設定する前にディセーブルになった場合、**participate** コマンドを入力する（または、ASDM で、[Participate in Load Balancing Cluster] チェックボックスをオンにする）と、エラー メッセージが表示され、そのクラスタに対する暗号化はイネーブルになりません。

クラスタの暗号化を使用するには、内部インターフェイスを指定して **crypto isakmp enable** コマンドを使用し、内部インターフェイス上の ISAKMP をイネーブルにする必要があります。

ステップ 5　クラスタの暗号化をイネーブルにする場合、**cluster key** コマンドを入力して IPsec 共有秘密情報も指定する必要があります。このコマンドは、IPsec 暗号化をイネーブルにしてある場合、IPsec ピア間に共有秘密を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。

```
hostname(config-load-balancing)# cluster key shared_secret
hostname(config-load-balancing)#
```

たとえば、共有秘密情報を 123456789 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

ステップ 6　participate コマンドを入力して、クラスタへのこのデバイスの参加をイネーブルにします。

```
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

完全修飾ドメイン名を使用したリダイレクションのイネーブル化

VPN ロードバランシング モードで完全修飾ドメイン名を使用したリダイレクトをイネーブルまたはディセーブルにするには、グローバル コンフィギュレーション モードで **redirect-fqdn enable** コマンドを使用します。この動作は、デフォルトではディセーブルになっています。

デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、その証明書はバックアップ デバイスにリダイレクトされたときに無効になります。

VPN クラスタ マスターとして、ASA は、VPN クライアント接続を別のクラスタ デバイスにリダイレクトする場合に、DNS 逆ルックアップを使用して、そのクラスタ デバイス（クラスタ内の別の ASA）の外部 IP アドレスではなく Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を送信できます。

クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

IP アドレスではなく、FQDN を使用して SSL 接続または IPsec/IKEv2 接続のロード バランシングを実行するには、次の設定手順を実行します。

ステップ 1　**redirect-fqdn enable** コマンドを使用して、ロード バランシングのための FQDN の使用をイネーブルにします。

redirect-fqdn {enable | disable}
no redirect-fqdn {enable | disable}

例：
```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)#
```

ステップ 2　DNS サーバに、各 ASA outside インターフェイスのエントリを追加します（エントリが存在しない場合）。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。

ステップ 3　**dns domain-lookup inside** コマンドを使用して、ASA で DNS ルックアップをイネーブルにします。inside の部分には、DNS サーバへのルートを持つ任意のインターフェイスを指定します。

ステップ 4　ASA 上の DNS サーバ IP アドレスを定義します。たとえば、**dns name-server 10.2.3.4**（DNS サーバの IP アドレス）。

次に、完全修飾ドメイン名のリダイレクトをイネーブルにし、クラスタのパブリック インターフェイスを **test** と指定し、クラスタのプライベート インターフェイスを **foo** と指定するインターフェイス コマンドを含む、VPN ロードバランシング コマンド シーケンスの例を示します。

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

```
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

ロード バランシングについての FAQ

IP アドレス プールの枯渇

Q : ASA は、IP アドレス プールの枯渇をその VPN ロードバランシング方式の一部と見なしますか。

A : いいえ。リモート アクセス VPN セッションが、IP アドレス プールが枯渇したデバイスに転送された場合、セッションは確立されません。ロードバランシング アルゴリズムは、負荷に基づき、各バックアップ クラスタ メンバが提供する整数の割合（アクティブ セッション数および最大セッション数）として計算されます。

固有の IP アドレス プール

Q : VPN ロード バランシングを実装するには、異なる ASA 上の AnyConnect クライアントまたは IPsec クライアントの IP アドレス プールを固有にする必要がありますか。

A : はい。IP アドレス プールはデバイスごとに固有にする必要があります。

同じデバイスでのロード バランシングとフェールオーバーの使用

Q : 単一のデバイスで、ロード バランシングとフェールオーバーの両方を使用できますか。

A : はい。この設定では、クライアントはクラスタの IP アドレスに接続し、クラスタ内で最も負荷の少ない ASA にリダイレクトされます。そのデバイスで障害が発生すると、スタンバイ装置がすぐに引き継ぎ、VPN トンネルにも影響を及ぼしません。

複数のインターフェイスでのロード バランシング

Q : 複数のインターフェイスで SSL VPN をイネーブルにする場合、両方のインターフェイスにロード バランシングを実装することはできますか。

A : パブリック インターフェイスとしてクラスタに参加するインターフェイスは 1 つしか定義できません。これは、CPU 負荷のバランスをとることを目的としています。複数のインターフェイスは、同じ CPU に集中するため、複数のインターフェイスにおけるロード バランシングの概念には意味がありません。

ロード バランシング クラスタの最大同時セッション

Q : それぞれが 100 ユーザの SSL VPN ライセンスを持つ 2 つの ASA 5520 が構成されているとします。この場合、ロードバランシング クラスタで許可されるユーザの最大合計数は、200 同時セッションでしょうか。または 100 同時セッションだけでしょうか。さらに 100 ユーザ ライセンスを持つ 3 台目のデバイスを追加した場合、300 の同時セッションをサポートできますか。

A : VPN ロード バランシングを使用すると、すべてのデバイスがアクティブになるため、クラスタでサポートできる最大セッション数は、クラスタ内の各デバイスのセッション数の合計になります。この例の場合は、300 になります。

ロード バランシングの表示

ロードバランシング クラスタのマスターは、アクティブな AnyConnect セッション、クライアントレス セッション、そして設定された制限またはライセンス数制限に基づく最大許可セッションがあるクラスタ内の各 ASA からメッセージを定期的に受信します。クラスタ内のある ASA の容量が 100% いっぱいであると示される場合、クラスタ マスターはこれに対してさらに接続をリダイレクトすることはできません。ASA がいっぱいであると示されても、ユーザによっては非アクティブまたは再開待ち状態となり、ライセンスを消費する可能性があります。回避策として、セッション合計数ではなく、セッション合計数から非アクティブ状態のセッション数を引いた数が各 ASA によって提供されます（コマンド リファレンスの **-sessiondb summary** コマンドを参照してください）。つまり、非アクティブなセッションはクラスタ マスターに報告されません。ASA が（非アクティブなセッションによって）いっぱいになっている場合でも、クラスタ マスターは必要に応じて接続を ASA に引き続きリダイレクトします。ASA が新しい接続を受信すると、最も長く非アクティブになっていたセッションがログオフされ、新しい接続がそのライセンスを引き継ぎます。

次の例は、100 個の SSL セッション（Active のみ）と 2% の SSL 負荷を示しています。これらの数字には、非アクティブなセッションは含まれていません。つまり、非アクティブなセッションはロードバランシングの負荷に数えられません。

```
hostname#  load-balancing
    Status :       enabled
    Role :         Master
    Failover :     Active
    Encryption :   enabled
    Cluster IP :   192.168.1.100
    Peers :        1

                                                Load %
Sessions
    Public IP      Role    Pri     Model          IPsec   SSL     IPsec SSL
    192.168.1.9    Master  7       ASA-5540       4       2       216     100
    192.168.1.19   Backup  9       ASA-5520       0       0       0       0
```

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情報を示しています。

```
hostname(config)# show version

Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)

Compiled on Sun 02-Jan-11 03:45 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "startup-config"
asa4 up 9 days 3 hours

Hardware:   ASA5510, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz
Internal ATA Compact Flash, 256MB
BIOS Flash M50FW080 @ 0xfff00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode        : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode     : CNLite-MC-SSLm-PLUS-2.03
```

```
                            IPsec microcode       : CNlite-MC-IPSECm-MAIN-2.06
                            Number of accelerators: 1

 0: Ext: Ethernet0/0         : address is 001e.f75e.8b84, irq 9
 1: Ext: Ethernet0/1         : address is 001e.f75e.8b85, irq 9
 2: Ext: Ethernet0/2         : address is 001e.f75e.8b86, irq 9
 3: Ext: Ethernet0/3         : address is 001e.f75e.8b87, irq 9
 4: Ext: Management0/0       : address is 001e.f75e.8b83, irq 11
 5: Int: Internal-Data0/0    : address is 0000.0001.0002, irq 11
 6: Int: Internal-Control0/0 : address is 0000.0001.0001, irq 5

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 100            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 2              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 250            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has an ASA 5510 Security Plus license.

hostname#
```

AnyConnect VPN セッション（IPsec/IKEv1 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。

たとえば、ASA のライセンスで 500 の AnyConnect VPN セッションが許可されていて、SSL 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** 形式を使用します。

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

Cisco VPN Client（IPsec IKEv1）、LAN-to-LAN VPN、およびクライアントレス SSL VPN のセッション数を ASA が許可してい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 max-other-vpn-limit** コマンドを入力します。

たとえば、ASA のライセンスが 750 の IPsec セッションを許可していて、IPsec セッション数を 500 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-other-vpn-limit 500
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-other-vpn-limit 500
hostname(config)#
```

各ライセンスで使用できる機能の詳細については、次の URL にある『Managing Feature Licenses for Cisco ASA 5500 Version 8.4』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa84/license_standalone/license_management/license.html

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と、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

AnyConnect TLS/DTLS トラフィックに対してより適切なスループット パフォーマンスが得られるように、対称型マルチプロセッシング（SMP）プラットフォーム上での暗号化コアの割り当てを変更することができます。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。

（注） マルチ コンテキスト モードが適用されるのは、IKEv2 および IKEv1 のサイトツーサイトのみであり、AnyConnect、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、および IKEv1 IPsec の cTCP には適用されません。

制限事項

- 暗号化コア再分散ができるのは、次のプラットフォームです。
  - 5585-X
  - 5580

- 5545-X
- 5555-X
- ASASM

• ラージ モジュラス演算を使用できるのは、5510、5520、5540、および 5550 プラットフォームだけです。

手順の詳細

	コマンド	目的
ステップ 1	`asa1(config)# crypto engine ?` `asa1(config)# crypto engine accelerator-bias ?`	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。 • balanced：暗号ハードウェア リソースを均等に分散します。 • ipsec：暗号ハードウェア リソースを優先 IPSec/暗号化音声（SRTP）に割り当てます。 • ssl：暗号ハードウェア リソースを優先 SSL に割り当てます。
ステップ 2	`large-mode-accel`	ハードウェアでラージ モジュラス演算を実行します。

アクティブな VPN セッションの表示

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。

コマンド	目的
`show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}`	このコマンドは、エンドポイントのパブリック 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 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 a-ipversion {v4 | v6}`	このコマンドは、エンドポイントの割り当て済み 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。

例

例 3-1　show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6] コマンドの出力

```
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
```

例 3-2　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。

コマンド	目的
show vpn-sessiondb webvpn filter ipversion {v4 | v6}	このコマンドは、エンドポイントのパブリック 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クライアントレス SSL 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。

例

例 3-3　show vpn-sessiondb webvpn filter ipversion [v4 | v6] コマンドの出力

```
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。

コマンド	目的
show vpn-sessiondb l2l filter ipversion {v4 | v6}	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。