CHAPTER 29

IPSec/SSL VPN の一般パラメータの設定

バーチャル プライベート ネットワークのセキュリティ アプライアンスの実装には、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。

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 モードでのセキュリティ アプライアンスへの接続（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 IPSec/SSL の設定

（注） クライアントレス（ブラウザモード）SSL VPN が指定されていない限り、この章の SSL VPN の語は、SSL VPN クライアント（AnyConnect 2.x または以前の SVC 1.x）を指します。

IPSec/SSL 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/SSL 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、セキュリティ アプライアンスの背後で別の VPN コンセントレータを使用し、なおかつセキュリティ アプライアンスのパフォーマンスを最大限にする場合などです。通常、IPSec/SSL 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、セキュリティ アプライアンス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、ACL をチェックせずにセキュリティ アプライアンスを通過する IPSec/SSL トラフィックをイネーブルにします。

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

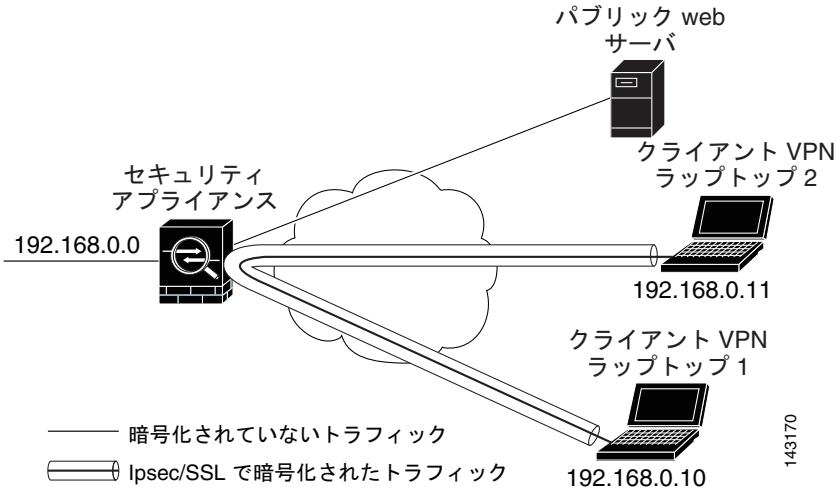
インターフェイス内トラフィックの許可（ヘアピニング）

セキュリティ アプライアンスには、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（セキュリティ アプライアンス）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、この機能により、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 29-1 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/SSL 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 29-1　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/SSL 接続に固有ではありません。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 規則をセキュリティ アプライアンス 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

セキュリティ アプライアンス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)# global (outside) 1 interface
hostname(config)# nat (outside) 1 192.168.0.0 255.255.255.0
```

ただし、セキュリティ アプライアンス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)# access-list nonat permit ip 192.168.0.0 255.255.255.0 192.168.0.0
255.255.255.0
hostname(config)# nat (outside) 0 access-list nonat
```

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/SSL VPN セッションの最大数の設定

VPN セッションの数をセキュリティ アプライアンス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 max-session-limit** コマンドを入力します。

- このコマンドは、SSL VPN（AnyConnect とクライアントレス）を含むあらゆるタイプの VPN セッションに適用されます。
- 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。

構文は、**vpn-sessiondb max-session-limit {***session-limit***}** です。

次に、最大 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-session-limit 450
hostname (config)#
```

SSL VPN クライアントおよびクライアントレス最大セッション数の両方を設定するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-webvpn-session-limit {***session-limit***}** コマンドを入力します。

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

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 タイプにだけ適用されます。

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、client-update 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更新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、セキュリティ アプライアンス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 client-update 値を指定します。

これを行うコマンドの構文は次のとおりです。

```
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。リビジョン番号は 4.6.1、アップデートを取得するための URL は https://support/updates を指定しています。

```
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 モードに入ると、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。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 グループに対して client-update パラメータのセットを定義するには、次の手順を実行します。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、Windows クライアントなどのクライアントをアップデートする必要はありません。

```
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　オプションで、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できます。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。

ロード バランシングの概要

リモート セッションを処理するために同じネットワークに接続されている 2 つ以上のセキュリティ アプライアンスまたは 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*セカンダリ 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、クラスタ内のセカンダリ 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。

（注）　**show** コマンドの出力は、クラスタ内のセカンダリ デバイスをバックアップ デバイスとして表示する場合があります。

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 Client 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）　すべての Cisco IPsec クライアント（ソフトウェアおよび VPN 3002、PIX-501、IOS 800 シリーズ、ASA 5505 ハードウェア クライアント）と SSL VPN クライアント。

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、クラスタ内のセカンダリ 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/SSL 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。これらの値は、クラスタ内のすべてのデバイスに対して同一に設定する必要があります。
- 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。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。

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。

ロード バランシング アルゴリズム

ロード バランシングはユーザ負荷率によって計算されます。アプライアンスの違いに伴うプリファレンスはありません。ユーザ負荷率がロード バランシングに関して考慮される唯一の要素です。ユーザの負荷率をあるアプライアンスでより早く増加させる場合、この特定のアプライアンスがサポートできるユーザの最大数を設定する必要があります。ユーザの最大数（5000）をサポートするように設定した場合、負荷の 1 % に相当するには 50 人のユーザが必要なことに注意してください。

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 5520 以降のセキュリティ アプライアンス モデル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。

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 VPN Client（Release 3.0 以降）
- Cisco VPN 3002 Hardware Client（Release 3.5 以降）
- Cisco PIX 501/506E（Easy VPN クライアントとして動作している場合）。
- Cisco AnyConnect VPN Client（Release 2.0 以降）
- Cisco ASA 5505 セキュリティ アプライアンス（Easy VPN クライアントとして動作する場合）
- IKE リダイレクトをサポートする IOS EZVPN クライアント デバイス（例：IOS 831/871）
- クライアントレス SSL VPN（ブラウザモード。クライアントではない）

ロード バランシングは、IPSec/SSL クライアント セッションと SSL VPN（AnyConnect とクライアントレス）セッションの両方で機能します。その他すべてのクライアント（LAN-to-LAN 接続を含む）は、ロード バランシングがイネーブルになっているセキュリティ アプライアンスに接続できますが、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 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、すべてが ASA Release 7.0(x) セキュリティ アプライアンス、すべてが ASA Release 7.1(1) セキュリティ アプライアンス、すべてが VPN 3000 コンセントレータ、またはこれらの混在で構成することができます。次の制限があります。

- すべてが ASA 7.0(x) セキュリティ アプライアンス、すべてが ASA 7.1(1) セキュリティ アプライアンス、またはすべてが 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 クラスタでは、IPSec/SSL セッションおよび SSL VPN（AnyConnect とクライアントレス）セッションの混在に対してロード バランシングを実行できます。
- ASA 7.0(x) セキュリティ アプライアンスと 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/SSL および SSL VPN（AnyConnect およびクライアントレス）セッションの混在に対してロード バランシングを実行できます。
- ASA 7.1(1) セキュリティ アプライアンス、および ASA 7.0(x) または VPN 3000 コンセントレータのいずれか、もしくは両方を含むロード バランシング クラスタは、IPSec/SSL セッションだけ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 7.1(1) セキュリティ アプライアンスは、それぞれの IPSec/SSL 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（AnyConnect およびクライアントレス）接続なしの混在クラスタ」（P.9）に、この状況を示します。

リリース 7.1(1) を使用すると、IPSec/SSL セッションと SSL VPN（AnyConnect およびクライアントレス）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 コンセントレータ用のロード バランシングの計算からの逸脱を意味しています。つまり、これらのプラットフォームは、一部のハー

ドウェア プラットフォームにおいて、IPSec/SSL セッションの負荷とは別に、SSL VPN（AnyConnect およびクライアントレス）セッションの負荷を計算する重み付けアルゴリズムを使用しています。

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 Release 7.1(1) セキュリティ アプライアンスでは、SSL VPN（AnyConnect およびクライアントレス）または IPSec/SSL のすべてのセッションを同等と見なし、それらのセッションを適宜割り当てます。ASA Release 7.0(x) セキュリティ アプライアンスまたは VPN 3000 コンセントレータでは、セッションの負荷を割り当てるときに重み付け計算を実行します。

（注）　許可する IPSec/SSL セッションと SSL VPN（AnyConnect およびクライアントレス）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」（P.29-13）を参照してください。

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) および VPN 3000 コンセントレータを実行しているセキュリティ アプライアンスが少なくとも 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セキュリティ アプライアンスと 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（AnyConnect およびクライアントレス）接続なしの混在クラスタ

このシナリオでは、クラスタはセキュリティ アプライアンスと VPN 3000 コンセントレータの混在で構成されています。セキュリティ アプライアンス 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) よりも前のピアおよび 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があり、2 つの SSL VPN（AnyConnect およびクライアントレス）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/SSL 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（AnyConnect およびクライアントレス）ライセンスは、ユーザの最大 IPSec/SSL 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、混在クラスタ内のセキュリティ アプライアンスの SSL VPN（AnyConnect およびクライアントレス）ライセンスの数が少なければ少ないほど、IPSec/SSL セッションしかないシナリオで IPSec/SSL 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（AnyConnect およびクライアントレス）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セキュリティ アプライアンスが最初のクラスタ 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/SSL および SSL VPN（AnyConnect およびクライアントレス）セッションの負荷の組み合わせを、先行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) セキュリティ アプライアンス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、クラスタがセキュリティ アプライアンスと 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。セキュリティ アプライアンス 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、クラスタでは SSL VPN 接続だけでなく IPSec/SSL 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。本質的に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お勧めします。

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。

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、セキュリティ アプライアンスにパブリック 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、セキュリティ アプライアンスにプライベート 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。

```
hostname(config-load-balancing)# nat ip_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 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
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 アドレスを指定します。仮想クラスタ内のすべてのセキュリティ アプライアンスが共有しているパブリック サブネット アドレスの範囲内にある IP アドレスを選択します。

```
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 192.168.10.10 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 192.168.10.10
hostname(config-load-balancing)#
```

ステップ 3　クラスタ ポートを設定します。このコマンドは、このデバイスが参加している仮想クラスタの 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　オプションで、クラスタに対する IPSec/SSL 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/SSL 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。仮想クラスタ内のセキュリティ アプライアンスは、IPSec/SSL 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内部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/SSL 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/SSL 暗号化をイネーブルにしてある場合、IPSec/SSL ピア間に共有秘密情報を指定します。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)#
```

VPN セッション制限の設定

IPSec/SSL セッションと SSL VPN（AnyConnect およびクライアントレス）セッションは、セキュリティ アプライアンスのプラットフォームと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。セキュリティ アプライアンスの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抜粋した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 7.1(0)182
Device Manager Version 5.1(0)128

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs               : 100
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Security Contexts           : 10
GTP/GPRS                    : Enabled
VPN Peers                   : 750
SSLVPN Peers                : 500

This platform has an ASA 5520 VPN Plus license.
```

アクティブな IPSec/SSL VPN セッションの最大数をセキュリティ アプライアンス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-session-limit** コマンドを入力します。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。

```
hostname(config)# vpn-sessiondb max-session-limit number_of_sessions
hostname(config)#
```

たとえば、セキュリティ アプライアンスのライセンスで 750 の IPSec/SSL セッションが許可されていて、IPSec/SSL 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-session-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-session-limit
hostname(config)#
```

SSL VPN（AnyConnect およびクライアントレス）セッションをセキュリティ アプライアンス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-webvpn-session-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。

```
hostname(config)# vpn-sessiondb max-webvpn-session-limit number_of_sessions
hostname(config)#
```

たとえば、セキュリティ アプライアンスのライセンスで 500 の SSL VPN（AnyConnect およびクライアントレス）セッションが許可されていて、SSL VPN（AnyConnect およびクライアントレス）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-webvpn-session-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-webvpn-session-limit
hostname(config)#
```

各ライセンスで使用できる機能の詳細については、付録 A「機能のライセンスと仕様」を参照してください。

全体的な考慮事項

この項では、VPN ロード バランシングを設定する際に考慮する必要のある質問と回答を示します。

Q. ASA は、IP プールの枯渇をその VPN ロード バランシング メカニズムの一部と見なしますか。

A. いいえ。VPN リモート アクセス セッションが IP プールが枯渇した最も負荷の少ない装置に転送された場合、セッションは確立に失敗します。アルゴリズムは負荷に基づいており、各セカンダリ クラスタ メンバにより提供される整数の割合（アクティブ / 最大セッションの数）として計算されます。

Q. ASA 自身の内蔵ロード バランシングで VIP を使用しているクラスタには 4 つの ASA があります。クラスタの 4 つのメンバすべてで同じグループ URL を問題なく使用できますか。また、DNS の見地からして、VIP を指す A レコードだけを作成できますか。または他に何かをする必要がありますか。

A. 各クラスタ メンバで **group-url https://vpn.rob.com/eng enable** を使うことはできません。代わりに、ASA の実際の IP アドレス（VIP ではない）を使用する必要があります。URL または VIP IP、あるいはその両方を使用すると、AnyConnect は接続できません。

例 : 2 つ ASA があるクラスタ セットアップがあり、グループ URL に FQDN と IP アドレスの両方があることが判明しました。クラスタにアクセスしようとすると、ASA はクラスタ内のマシンの IP アドレスを使用します。FQDN グループ URL を削除し、その動作が停止しました。

ASA1 のグループ URL は、**group-url https://10.94.147.93/BasicGroup**

および

ASA2 のグループ URL は、**group-url https://10.94.147.92/BasicGroup**

そうすると、クラスタ名とグループ URL（**cvc-asa.cisco.com/BasicGroup**）を使用して、クラスタおよび BasicGroup にアクセスできます。

Q. VPN ロード バランシングを実装する際に、クラスタに参加している異なる ASA 上の AnyConnect クライアント（または IPSec/SSL クライアント）のアドレス プールは異なってはいけませんか。

A. そのとおりです。アドレス プールを使用する場合、デバイスごとに一意である必要があります

Q. ロード バランシングおよびフェールオーバーを組み合わせることはできますか。

A. はい。

ロード バランシングとフェールオーバーの両方を組み合わせる設定もできます。たとえば、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 ASA がダウンすると、スタンバイ装置がすぐに引き継ぎ、クライアントのトンネルにも影響を及ぼしません。

（注）　アクティブ装置だけがロード バランシングに参加します。フェールオーバーのペアのアクティブ装置がダウンした場合、そのスタンバイ装置がアクティブになり、VPN セッションの負荷を分散させるためにロード バランシング クラスタ メカニズムに参加します。

Q. 複数のインターフェイスでイネーブルになっている SSL VPN（AnyConnect およびクライアントレス）がある場合、これら両方に対して VPN 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ように定義できるのは、1 台のインターフェイスだけです。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でも同じ CPU に集中することに変わりはないため、インターフェイス間のロードバランシングの概念に価値はありません。現時点でこれをサポートする予定はありません。

Q. デフォルトでクラスタ マスターが着信接続をリダイレクトする場合、IP アドレスによってリダイレクトするため、FQDN ではなく IP アドレスとともに ASA に表示されます。

A. オプションで、ローカル ASA にグループ URL https://ip_address/group-url を追加するか、次のコマンドを ASA に追加して、IP アドレスよりも FQDN で転送するようにできます。

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

Q. SSL ライセンスおよびフェールオーバーを実装しようとする場合、次の導入を検討します。

1 つのロード バランシング クラスタに 2 つの ASA5520（それぞれに 100 ユーザの SSL VPN ライセンスが付属）。

ユーザの最大合計数では、200 人のユーザが同時に許可されますか、または最大 100 人だけが許可されますか。100 人のユーザの 3 台目のデバイスを後で追加した場合、300 人のユーザを同時にサポートできるようになりますか。

A. VPN ロード バランシングでは、すべてのデバイスがアクティブになります。これにより、デバイスごとにライセンスされた数が使用できるようになります。クラスタがサポートできるユーザの最大数を決定するためにこれらを合算します。この例では、2 つの ASA の場合は 200 セッション、また 3 つの ASA の場合は 300 セッションとなります。

Q. ロード バランシング クラスタリングに参加できるアプライアンスの数に制限はありますか。

A. ハード制限はありません。1 つのクラスタで最大 10 ノードまでエンジニアリング テストを行っています。より多くのノードでも動作する可能性はありますが、公式にそのトポロジをサポートしていません。

Q. ロード バランシングは適応型セキュリティ アプライアンスに対してどのように動作しますか。

A. 基本的には、ロード バランシングは、次のように動作します。

- フェーズ 1 のネゴシエーションは、仮想マスターで実行されます。
- スレーブ デバイスの IP の IKE リダイレクト パケットが仮想マスターからクライアントに送信されます。

- クライアントは、新しいフェーズ 1 およびフェーズ 2 のネゴシエーションをスタンドアロン VPN 接続と同じようにスレーブ デバイスで開始します。

リモート アクセスの場合、ルートを手動で設定する必要はありません。この状況は、スタンドアロンの場合も、ロード バランシングによってリダイレクトされたトンネルの場合も同じです。基本的に、クライアント デバイスのパブリック IP を指す、割り当て済み IP アドレスのホスト ルートは、ASA の内部インターフェイスにインストールされます。「show route」は、ホスト ルートを表示します。この逆ルートにより、ASA の内部インターフェイスは、クライアントの割り当て済み IP の ARP 要求に応答するため、内部ネットワーク上のサーバからトンネルを介してクライアントにトラフィックを返すことができます。

ロード バランシングは、IPSec/SSL ハードウェア クライアント（VPN3002、PIX501、ASA5505）のクライアント/PAT モードおよびネットワーク拡張モード（NEM）でも動作します。