IPSec 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。ここでは、次の項目について説明します。

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 Active/Active 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、透過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-ipsec** 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、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 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。

シンタックスは、**sysopt connection permit-ipsec** 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 をチェックせずにセキュリティ アプライアンスを通過する IPSec トラフィックをイネーブルにします。

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

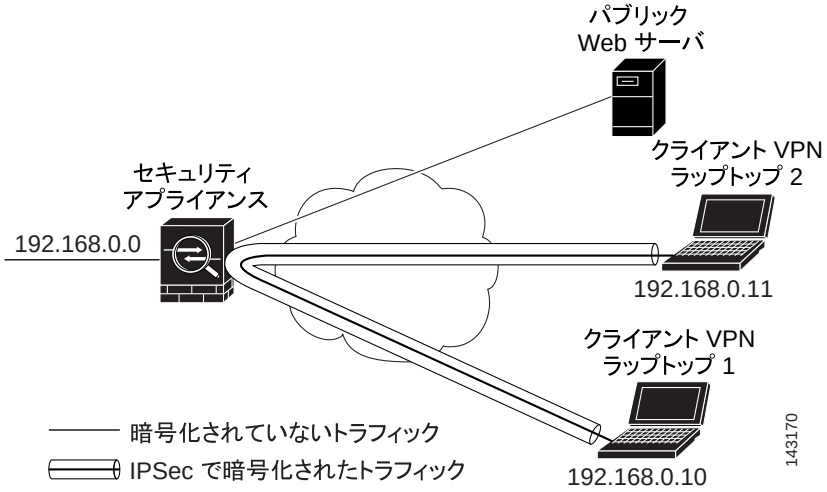
インターフェイス内トラフィックの許可

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 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。

コマンドのシンタックスは、**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」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 規則を適用しています。

```
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 規則の詳細については、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 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、WebVPN 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。

シンタックスは、**vpn-sessiondb max-session-limit {***session-limit***}** です。

次の例では、VPN セッションの最大数を 450 に設定する方法を示しています。

```
hostname (config)# vpn-sessiondb max-session-limit 450
hostname (config)#
```

許可されるクライアント 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もあります。**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、アップデートが適用され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、オプションとして 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 クライアントの場合は、アップデート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 クライアントのユーザの場合、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 トンネルグループのタイプだけに適用されます。

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 アトリビュート 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。クライアントがリビジョン番号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場合、ソフトウェアをアップデートする必要はありません。クライアントが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場合、アップデート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です。

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、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、アップデートされたイメージを取得する URL または IP アドレス、およびそのクライアントの許可されるリビジョン番号を指定します。リビジョン番号は、カンマで区切って最大 4 つまで指定できます。

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。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シンタックスは次のとおりです。

```
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。

クライアントがリビジョン番号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場合、ソフトウェアをアップデートする必要はありません。クライアントが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場合、アップデート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*** は、許可されるすべての Windows プラットフォームを網羅します。***windows*** を指定する場合は、個々の Windows クライアント タイプは指定しません。

（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は、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専用にクライアント アップデートを設定できます（手順 3 を参照）。

VPN 3002 クライアントは、ユーザの介入なしにアップデートされるため、ユーザは通知メッセージを受け取りません。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。トンネルグループの ipsec アトリビュート 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」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。ここでは、リビジョン番号 4.7 を指定し、アップデートされたソフトウェアを IP アドレス 192.168.1.1 のサイトから取得するために TFTP プロトコルを使用します。

```
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） たとえば **https://support/updates/vpnclient.exe** のように、URL の最後にアプリケーション名を含めると、ブラウザは自動的にアプリケーションを起動します。

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。トンネルグループの ipsec アトリビュート 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は、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　オプションとして、クライアントのアップデートが必要な旧式の Windows クライアントを持つ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 に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を提供します。このメッセージのうち設定できる部分は URL だけです（手順 2 または 3 を参照してください）。アクティブでないユーザは、次にログインしたときに通知メッセージを受け取ります。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な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することができます。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なクライアントに通知するには、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、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、ユーザの介入なしにアップデートされるため、ユーザは通知メッセージを受け取りません。

（注）　client-update タイプを ***windows*** として指定（すべての Windows ベースのプラットフォームを指定）した後、同じエントリに ***win9x*** または ***winnt*** の client-update タイプを入力する場合、最初にこのコマンドの **no** 形式を使用して windows クライアント タイプを削除してから、新しく client-update コマンドを使用して新しいクライアント タイプを指定する必要があります。

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上に接続されている 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、これらのデバイスは、セッション ロードを共有するように設定できます。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*としてグループ化します。

仮想クラスタ内のすべてのデバイスはセッション ロードを伝送します。ロードバランシングは、クラスタ内で最もロードの低いデバイスにセッショントラフィックを転送して、ロードをすべてのデバイス間で分散します。これにより、システム リソースが効率的に使用され、パフォーマンスの向上と高い可用性がもたらされます。

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監視し、各デバイスのビジー状態を把握して、適宜セッション ロードを分散します。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ことはなく、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 マスターが故障した場合、クラスタ内のセカンダリ デバイスがその役割を引き継いで、ただち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単一の*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。これは、現在の仮想クラスタ マスターに属しているため、仮想です。接続を確立しようと試みる 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、クラスタ内でロードが最小の使用可能なホストのパブリック IP アドレスをクライアントに送り返します。クライアントは、第 2 のトランザクション（ユーザには意識されない）で、そのホストに直接接続します。このようにして、仮想クラスタ マスターは、リソース全体にわたって均一かつ効率的にトラフィックを転送します。

（注） Cisco VPN クライアントまたは 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、通常どおりにセキュリティ アプライアンス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に障害が発生すると、終了し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。その後、仮想クラスタ マスターは、これらの接続をクラスタ内の別のアクティブ デバイスに転送します。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 マスターの役割を自動的に引き継ぎます。たとえクラスタ内の複数のデバイスに障害が発生しても、ユーザは、クラスタ内のいずれか 1 つのデバイスが実行中で使用可能である限り、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 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で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化して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、デバイスごとに異なります。

（注）　VPN ロードバランシングには、アクティブな 3DES/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化する前に、この暗号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かった場合、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。

最初にパブリック（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** および **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である IP アドレス、暗号設定、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 5520 以上のセキュリティ アプライアンスを含めることができます。VPN 3000 シリーズ コンセントレータをクラスタに含めることもできます。混在のコンフィギュレーションは可能ですが、一般にクラスタが同種であれば管理は容易になります。

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 セッションだけに有効です。

- Cisco VPN クライアント（Release 3.0 以上）
- Cisco VPN 3002 ハードウェア クライアント（Release 3.5 以上）
- Easy VPN クライアントとして動作している場合、Cisco PIX 501/506E

ロードバランシングは、IPSec クライアントおよび WebVPN セッションの両方で機能します。LAN-to-LAN 接続を含む他のすべてのクライアントは、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参加することはできません。

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、次の制限に従って、すべての ASA Release 7.0(x) セキュリティ アプライアンス、すべての ASA Release 7.1(1) セキュリティ アプライアンス、すべての 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。

- すべての ASA 7.0(x) セキュリティ アプライアンス、すべての ASA 7.1(1) セキュリティ アプライアンス、またはすべての 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 および WebVPN 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 アプライアンスおよび 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 および WebVPN 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、またはその両方を含むロードバランシング クラスタは、IPSec セッションだけをサポートできます。しかし、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 IPSec キャパシティに完全に到達しない可能性もあります。P.29-11 の「シナリオ 1：WebVPN 接続のない混在クラスタ」に、この状況を示します。

Release 7.1(1) を使用すると、IPSec および WebVPN セッションは、クラスタ内の各デバイスが伝送するロード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。このことは、これらのプラットフォームが共に一部のハードウェア プラットフォーム上で IPSec セッション ロードとは異なる方法で WebVPN セッションロードを計算する重み付けアルゴリズムを使用するという点において、ASA Release 7.0(x) ソフトウェアおよび 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脱却を意味しています。

クラスタの仮想マスターは、クラスタのメンバー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 アプライアンスはすべてのセッション、WebVPN または IPSec を同等と見なし、これら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 コンセントレータは、セッション ロードを割り当てる際に重み付け計算を実行します。

（注）　IPSec および WebVPN セッションの数は、コンフィギュレーションとライセンスで許可されている最大数まで設定できます。これら制限の設定方法については、P.29-15 の「VPN セッション制限の設定」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

混在の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 ASA ソフトウェア リリースの混在を実行しているデバイス、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 マスターに障害が発生して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相異が問題になります。

次のシナリオは、ASA Release 7.1(1) および 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：WebVPN 接続のない混在クラスタ

このシナリオでは、クラスタはセキュリティ アプライアンスおよび VPN 3000 コンセントレータの混在で構成されます。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) 以前の VPN 3000 ピアには、SSL VPN 接続がなく、7.1(1) クラスタ ピアは、2 つの WebVPN セッションを許可する基本 SSL VPN ライセンスだけを備えていますが、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 WebVPN ライセンスは、ユーザの最大 IPSec セッション制限の利用にはほんのわずかな影響しか及ぼしません。またそれは VPN 3000 コンセントレータがクラスタ マスターである場合に限られます。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 WebVPN ライセンスの数が少なくなると、それに応じて IPSec セッションしかないシナリオにおいてその IPSec セッションの制限に到達できる 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：WebVPN 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 マスターであり、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マスターを自動的に引き継ぎ、クラスタ内のプロセッサ ロードを決定するためにそのデバイス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 ロードを重み付けすることができません。したがって、クラスタ マスターは、IPSec および WebVPN セッション ロードの組み合せを、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) セキュリティ アプライアンスにロードを適切に割り当てられません。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 アプライアンスおよび 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、前述のシナリオと類似しています。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。しかし、この場合、クラスタは SSL VPN 接続だけでなく IPSec 接続も処理しています。

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、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、以前の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) 以前のピアにだけ適用されます。この場合、アクセスを拒否されることはありません。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、はるかにロードが軽くなっています。

しかし、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、問題が生じます。クラスタ マスターに障害が発生すると、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。結果が本質的に予測不能であるため、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の次の要素を設定します。

- パブリックおよびプライベート インターフェイス
- VPN ロードバランシング クラスタ アトリビュート

（注）　クラスタ内のすべての参加デバイスは、クラスタ内のデバイス プライオリティの場合を除いて、同一のクラスタ コンフィギュレーションを持つ必要があります。

ロードバランシング用のパブリックおよびプライベート インターフェイスの設定

ロードバランシング クラスタ デバイス用にパブリック（外部）およびプライベート（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。このコマンドは、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　クラスタ内のこのデバイスに割り当てるようにプライオリティを設定します。範囲は 1 ～ 10 です。プライオリティは、このデバイスが、起動時または既存のマスターに障害が発生したときに仮想クラスタ マスターになる可能性を示します。プライオリティを高く設定すると（たとえば 10）、それに応じてこのデバイスが仮想クラスタ マスターになる可能性も高くなります。

```
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 6 のプライオリティを割り当てるには、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　このデバイスのネットワーク アドレス変換を適用する場合は、デバイスの NAT 割り当て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 192.168.30.3 の NAT アドレスを割り当てるには、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 アトリビュートの設定

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 アトリビュートを設定するには、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 ロードバランシング コンフィギュレーション モードに移行し、ここで残りのロードバランシング アトリビュートを設定できます。

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。他のアプリケーションがこのポートを使用している場合は、ロードバランシングに使用する UDP 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、クラスタの 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。このチェックアトリビュートを設定する場合、最初に共有秘密情報を指定して確認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 を使用して LAN-to-LAN トンネルを介して通信します。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、このアトリビュート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、インターフェイス内でロードバランシングを事前に設定しておく必要があります。ロードバランシング内部インターフェイスでそのインターフェイスがイネーブルになっていない場合、クラスタ暗号化を設定しようと試みるとエラー メッセージが表示されます。

クラスタ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いたが、仮想クラスタへのデバイスの参加を設定する前にディセーブルにされた場合、**participate** コマンドを入力すると（または ASDM で Participate in Load Balancing Cluster チェックボックスを選択すると）エラー メッセージが表示され、そのクラスタに対して暗号化はイネーブルにはなりません。

クラスタ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 インターフェイスをイネーブルにする必要があります。

ステップ 5　クラスタ暗号化をイネーブルにする場合は、さらに **cluster key** コマンドを入力して IPSec 共有秘密情報を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、このデバイスのクラスタへ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 セッションおよび WebVPN 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およびライセンスがサポートする数だけ実行することができます。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。次の例で、コマンドと、このコマンドの出力からのライセンス情報の抜粋を示します。

```
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
WebVPN Peers                : 500

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

アクティブな IPSec 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 ライセンスが 750 の IPSec セッションを許可しており、IPSec セッションの数を 500 に制限したい場合は、次のコマンドを入力します。

```
hostname(config)# vpn-sessiondb max-session-limit 500
hostname(config)#
```

このセッション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)#
```

WebVPN 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-webvpn-session-limit** コマンドを使用します。このセッション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 ライセンスが 500 の WebVPN セッションを許可しており、WebVPN セッションの数を 250 に制限したい場合は、次のコマンドを入力します。

```
hostname(config)# vpn-sessiondb max-webvpn-session-limit 250
hostname(config)#
```

このセッション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)#
```

このライセンスで使用可能な機能の詳細な説明は、付録 A「機能のライセンスと仕様」を参照してください。