ロード バランシングの設定

この章では、ASDM を使用したロード バランシングの設定方法を説明します。この章には、次の項があります。

概要

リモート アクセス設定で、複数のセキュリティ アプライアンスまたは VPN コンセントレータが同じネットワークに接続されてリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担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 間ネットワーク、プライベート サブネット、パブリック サブネットにある複数のデバイスを 1 つの仮想クラスタに論理的にグループ化します。

仮想クラスタ内のすべてのデバイスが、セッション負荷を分担します。ロード バランシングは、セッションのトラフィックをクラスタ内の最も負荷の小さいデバイスに割り当てることによって、すべてのデバイス間に負荷を分散します。これにより、システム リソースが効率的に利用でき、パフォーマンスと可用性が向上します。

仮想クラスタ マスターと呼ばれる仮想クラスタ内の 1 つのデバイスが、セカンダリ デバイスと呼ばれる残りのデバイスに着信トラフィックを割り当てます。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、それぞれの作業負荷を追跡し、それに応じてセッション負荷を分散します。仮想クラスタ マスタの役割は、1 台の物理デバイスに固定されているのではなく、デバイス間で入れ替わることができます。たとえば、現在の仮想クラスタ マスターが故障すると、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ぎ、即座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からは、単一の仮想クラスタ IP アドレスとして認識されます。この IP アドレスは、特定の物理デバイスに固定されているわけではありません。これは、現在の仮想クラスタ マスターに所属します。つまり、仮想アドレスです。VPN クライアントが接続を確立しようとするとき、この仮想クラスタ IP アドレスにまず接続します。すると仮想クラスタ マスターは、クラスタ内の最も負荷の小さい利用可能なホストのパブリック IP アドレスをそのクライアントに送り返します。2 回目のトランザクションで、クライアントは直接そのホストに接続します（この動作はユーザには透過的です）。このように、仮想クラスタ マスターは、トラフィックを均一かつ効率的にリソース間に割り当てます。

（注） Cisco VPN Client、Cisco VPN 3002 Hardware Client、または Cisco ASA モデル 5505 以外のすべてのクライアントは、ハードウェア クライアントとして通常どおりセキュリティ アプライアンスに接続するよう設定されている場合は、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が故障してセッションが終了した場合、仮想クラスタ IP アドレスに即座に再接続できます。仮想クラスタ マスターは、次にこのような接続をクラスタ内の他のアクティブ デバイスに割り当てます。仮想クラスタ マスター自体が故障した場合、クラスタ内の他のデバイスが、即座に自動的に新しいセッション マスターになります。クラスタ内の複数のデバイスが故障した場合でも、クラスタ内のいずれか 1 つのデバイスが稼働し、利用可能である限り、ユーザは引き続きそのクラスタに接続できます。

ロード バランシングの実装

ロード バランシングを有効にするには、次の作業を行います。

- ロード バランシング クラスタの設定。共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタ用 IPSec 共有秘密鍵を確立します。これらの値は、クラスタ内のすべてのデバイスで同一です。
- 参加デバイスの設定。デバイス上でロード　バランシングを有効にし、デバイス固有のプロパティを定義します。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/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 バランシングを有効にする前に、この暗号化ライセンスが存在するかをチェックします。アクティブな 3DES または AES ライセンスを検出しない場合、ライセンスによってこの使用が許可されない限り、セキュリティ アプライアンスは、ロードバランシングの有効化を阻止するとともに、ロード バランシングシステムによる 3DES の内部設定を阻止します。

前提条件

ロード バランシングは、デフォルトで無効です。ロード バランシングは明示的に有効にする必要があります。

まず、パブリック インターフェイスとプライベート インターフェイスを設定するとともに、仮想クラスタ IP アドレスの参照先の仮想クラスタ IP のインターフェイスをあらかじめ設定する必要があります。

クラスタに参加するすべてのデバイスは、IP アドレス、暗号化設定、暗号化鍵、およびポートについて、クラスタ固有の値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、セキュリティ アプライアンス モデル ASA 5520 以上を使用できます。また VPN 3000 シリーズのコンセントレータも使用可能です。混合構成は可能ですが、一般に同種のクラスタの方が、管理が簡単です。

適格なクライアント

ロード バランシングは、次のクライアントが開始したリモート セッションでだけ有効です。

- Cisco VPN クライアント（リリース 3.0 以降）
- Cisco VPN 3002 ハードウェア クライアント（リリース 3.5 以降）
- Cisco ASA モデル 5505 （ハードウェア クライアントとして設定した場合）
- Cisco PIX 501/506E （Easy VPN として動作する場合）

IPSec クライアントと WebVPN セッションの両方と連係して動作するロード バランシング LAN 間接続を含む他のすべてのクライアントは、ロード バランシングが有効なセキュリティ アプライアンスに接続することはできますが、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 バランシングのクラスタ設定

ロード バランシング クラスタは、すべての ASA リリース 7.0（x）セキュリティ アプライアンス、すべての ASA リリース 7.1（1）セキュリティ アプライアンス以降、すべての VPN 3000 コンセントレータ、またはこれらを組み合せて構成できます。次の制約があります。

- すべての ASA 7.0（x）セキュリティ アプライアンス、ASA 7.1（1）セキュリティ アプライアンス以降、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 セッションと WebVPN セッションの組み合せに対してロード 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 セッションと WebVPN セッションの組み合せに対してロード バランシングを実行できます。
- ASA 7.1（1）セキュリティ アプライアンス以降と ASA 7.0（x）か VPN 3000 コンセントレータまたはその両方で構成されるロード バランシング クラスタは、IPSec セッションだけをサポートできます。ただしこのような構成では、ASA 7.1（1）以降のセキュリティ アプライアンスは最大の IPSec 能力を発揮できない場合もあります。P.11-5 の「シナリオ 1：WebVPN 接続のない混合クラスタ」に、この状況について示します。

リリース 7.1（1）以降では、クラスタ内の各デバイスの負荷の判定にあたって、IPSec セッションと WebVPN セッションの数や量が等しく測定されます。これは、ASA リリース 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大きく進歩した点です。これらの従来のプラットフォームでは、いずれも 1 つの WebVPN セッションを 10 の IPSec セッションと同じ負荷として計算する加重アルゴリズムを使用していました。

クラスタの仮想マスターは、セッション負荷をクラスタのメンバに割り当てます。ASA リリース 7.1（1）以降のセキュリティ アプライアンスは、すべてのセッション、Web VPN、IPSec、を等価と考え、そのように割り当てます。ASA リリース 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、セッション負荷の割り当てにおいて 10:1 の加重計算をします。

混合構成、つまりロード バランシング クラスタに、複数のリリースの ASA ソフトウェア、リリース 7.1（x）以降が動作する少なくとも 1 つのセキュリティ アプライアンス、および VPN 3000 コンセントレータが混在して動作している場合、最初のクラスタ マスターが故障して別のデバイスがマスターとして引き継いだときに、加重アルゴリズムの違いが問題となることがあります。

たとえば、ASA リリース 7.1（1）ソフトウェアが動作するセキュリティ アプライアンスが最初のクラスタ マスターであるとします。そしてそのデバイスが故障したとします。クラスタの別のデバイスが、自動的にマスターとして引き継ぎ、そのロード バランシング アルゴリズムを適用して、クラスタ内のプロセッサ負荷を判定します。しかし ASA リリース 7.1（1）ソフトウェアが動作するクラスタは、そのソフトウェアが提供する以外の方法で、セッション負荷を加重することができません。したがって、IPSec セッション負荷と WebVPN セッション負荷が混在している場合、旧バージョンが動作している ASA デバイスや VPN 3000 コンセントレータに対して、適切に負荷を割り当てられません。逆に、VPN 3000 コンセントレータがクラスタ マスターとして動作しているときは、ASA リリース 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られません。P.11-5 の「シナリオ 2：WebVPN 接続を処理する混合クラスタ」にこのジレンマを示します。

（注）　許容される IPSec セッションと WebVPN セッションの数は、構成とライセンスによって許可される最大数まで設定できます。このような制限を設定する方法については、P.11-8 の「VPN セッション制限の設定」を参照してください。

混合クラスタのシナリオ

次のシナリオは、ASA リリース 7.1（1）以降、ASA リリース 7.0（x）ソフトウェア、VPN 3000 シリーズ コンセントレータがそれぞれ動作するさまざまなセキュリティ アプライアンスが混在するクラスタで、VPN ロード バランシングを使用する方法を示します。

シナリオ 1：WebVPN 接続のない混合クラスタ

このシナリオでは、クラスタにセキュリティ アプライアンスと VPN 3000 コンセントレータが混在しています。セキュリティ アプライアンス クラスタの中には、ASA リリース 7.0（x）が動作するデバイスもあれば、リリース 7.1（1）以降が動作するデバイスもあります。7.1（1）より前リリースと VPN 3000 のデバイスには、SSL VPN 接続機能がまったくなく、7.1（1）以降のリリースのデバイスは、基本の SSL VPN ライセンスしかありません。したがって、2 つの Web VPN セッションは設定できますが、SSL VPN 接続は利用できません。この場合、すべての接続が IPSec となり、ロード バランシングが適切に機能します。

2 つの WebVPN ライセンスは、ユーザが IPSec のセッション制限を最大限まで利用することに関してほとんど影響を及ぼしません。またその影響は 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、IPSec セッションだけのシナリオでは、混合クラスタのセキュリティ アプライアンスにある Web VPN が少なければ少ないほど、ASA 7.1（1）以降のデバイスが IPSec のセッション制限に達する可能性が小さくなります。

シナリオ 2：WebVPN 接続を処理する混合クラスタ

このシナリオは、クラスタにセキュリティ アプライアンスと VPN 3000 コンセントレータが混在する上のシナリオと似ています。セキュリティ アプライアンス クラスタの中には、ASA リリース 7.0（x）が動作するデバイスもあれば、リリース 7.1（1）以降が動作するデバイスもあります。しかしこのケースでは、クラスタが IPSec 接続だけでなく、SSL VPN 接続も処理します。

ASA リリース 7.1（1）より前のソフトウェアが動作するデバイスがクラスタ マスターの場合、マスターが実際にはリリース 7.1（1）より前のプロトコルとロジックを適用することになります。つまり、そのセッション制限を超えているロード バランシング デバイスにセッションが割り当てられる可能性があります。この場合、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 リリース 7.0（x）ソフトウェアを実行するデバイスの場合、古いセッション加重アルゴリズムは、クラスタ内の 7.1（1）より前のデバイスにだけ適用されます。この場合、ユーザが拒否されることはありません。7.1（1）より前のデバイスはセッション加重アルゴリズムを使用するため、負荷が軽くなります。

ただし、クラスタ マスターが常に 7.1（1）以降のデバイスになることを保証できないという問題があります。クラスタ マスターが故障すると、他のデバイスがマスターの役割を引き継ぎます。新しいマスターには、適格なデバイスであれば、どれでもなれます。どのデバイスがマスターになるかを予見できないため、このタイプのクラスタ構成は避けることをお勧めします。

ロード バランシングの設定

ASA リリース 7.1（1）以降のソフトウェアが動作するセキュリティ アプライアンスでロード バランシングを設定するには、クラスタに参加する各デバイスに次の要素を設定します。

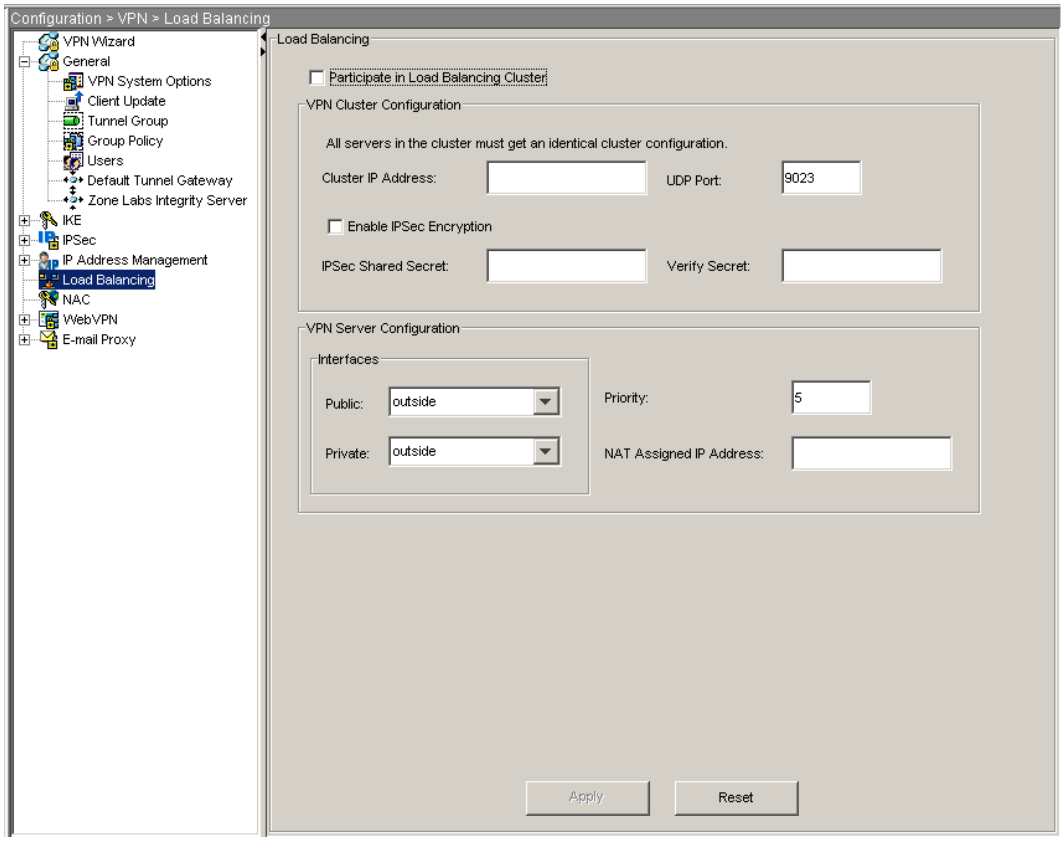
- パブリックとプライベートのインターフェイス
- VPN ロード バランシング クラスタ アトリビュート

（注）　クラスタのすべての参加デバイスには、クラスタ内のデバイスの優先順位を除き、同一のクラスタ設定を行う必要があります。

ロード バランシングのパブリックとプライベートのインターフェイスの設定

ロード バランシング クラスタを設定するには、**Configuration > VPN > Load Balancing** を選択します（図 11-1）。

図 11-1　Load Balancing ウィンドウ



ロード バランシングを設定する手順は、次のとおりです。

ステップ 1　Participate in Load Balancing チェックボックスをオンにします。

ステップ 2　VPN Cluster Configuration 領域で次のようにアトリビュートを設定します。

（注）　すべてのクラスタに同一のクラスタ設定を行う必要があります。

a. **Cluster IP Address** を入力します。これは、仮想クラスタ全体を表す単一の IP アドレスです。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。

b. **UDP Port** に、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 の宛先ポート番号を入力します。

c. オプションで、クラスタに対して IPSec の暗号化を有効にします。これには、**Enable IPSec Encryption** チェックボックスをオンにします。デフォルトでは、暗号化が無効です。このアトリビュートによって、IPSec の暗号化の有効と無効が切り替えられます。このアトリビュートを設定する場合、共有秘密鍵を指定し、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 間トンネル経由で通信を行います。デバイス間のすべてのロード バランシング情報が暗号化されるようにするには、この属性をオンにします。

（注）　暗号化を使用する場合は、ロード バランシングの内部インターフェイスをあらかじめ設定しておく必要があります。内部インターフェイスが有効でない場合は、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 バランシングの内部インターフェイスが有効でも、仮想クラスタのデバイスの参加を設定する前に無効にすると、Participate in Load Balancing Cluster チェックボックスを選択した時点でエラー メッセージが表示され、クラスタの暗号化を有効にできません。

d. クラスタの暗号化を有効にする場合は、IPSec の共有秘密鍵も指定する必要があります。これには、**IPSec Shared Secret** フィールドに値を入力してから、同じ値を **Verify Secret** フィールドに入力します。これらのフィールドには同一の値を設定する必要があります。これらのコマンドは、IPSec の暗号化を有効にしたときに、IPSec デバイス間の共有秘密鍵を指定します。このフィールドに入力した値は、一連のアスタリスクとして画面に表示されます。

ステップ 3　VPN Server Configuration 領域で次のようにアトリビュートを設定します。

a. **Public** で、セキュリティ アプライアンスのパブリック インターフェイスを選択します。このコマンドは、このデバイスのロード バランシングに使用するパブリック インターフェイスの名前または IP アドレスです。デフォルト値は outside です。

b. **Private** で、セキュリティ アプライアンスのプライベート インターフェイスを選択します。このコマンドは、このデバイスのロード バランシングに使用するプライベート インターフェイスの名前または IP アドレスです。デフォルト値は inside です。

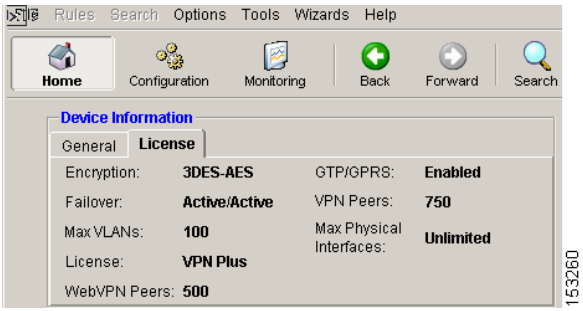
c. クラスタ内でこのデバイスに割り当てる優先順位を設定します。範囲は 1 ～ 10 です。この優先順位は、このデバイスが、起動時または他のマスターの故障時に仮想クラスタ マスターになる可能性を示します。優先順位を高く設定すれば（たとえば 10）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

d. ネットワーク アドレス変換をこのデバイスに適用する場合は、NAT Assigned IP Address に、NAT に割り当てられた IP アドレスを入力します。

VPN セッション制限の設定

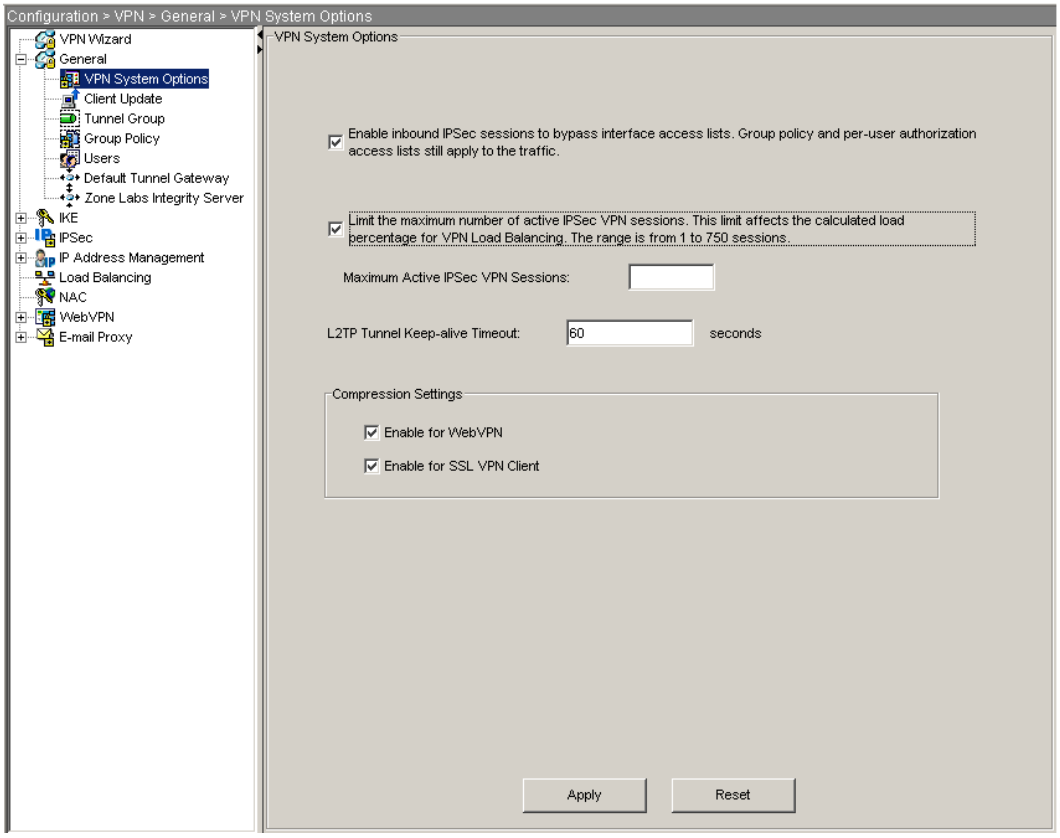
IPSec セッションと WebVPN セッションは、プラットフォームと セキュリティ アプライアンスのライセンスがサポートする限り、いくつでも実行できます。セキュリティ アプライアンスのライセンス情報を表示するには、ASDM の初期ウィンドウの上部にある Home アイコンを選択し、License タブを選択します（図 11-2）。

図 11-2　ライセンス情報



アクティブな IPSec VPN セッションの最大数を制限して、セキュリティ アプライアンスが許可している数より小さくするには、**Configuration > VPN > General > VPN System Options** を選択します（図 11-3）。

図 11-3　VPN System Options ウィンドウ



Maximum Active IPSec VPN Sessions フィールドに、適用する制限値を指定します。セッションの最大数は、ライセンスによって決まります。この制限は、VPN Load Balancing の負荷率の計算に影響を与えます。

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いて、IPSec セッション数を 500 に制限する場合は、**Maximum Active IPSec VPN Sessions** フィールドに 500 と入力します。

セッション制限を削除するには、**Limit the maximum number of active IPSec VPN sessions** チェックボックスをオフにします。

各種ライセンスで利用できる機能の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の付録 A「Feature Licenses and Specifications」を参照してください。