ハイアベイラビリティ オプション

ハイアベイラビリティ オプション

分散型 VPN クラスタリング、ロード バランシング、およびフェールオーバーは、それぞれ機能と要件が異なるハイアベイラビリティ機能です。状況によっては、複数の機能を導入環境で使用することがあります。以降では、これらの機能について説明します。分散型VPNとフェールオーバーの詳細については、『ASA General Operations CLI Configuration Guide』の適切なリリースを参照してください。ロード バランシングの詳細は以下に記載されています。

FXOS シャーシ上の VPN とクラスタリング

ASA FXOS クラスタは、S2S VPN に対する相互排他的な 2 つのモード（集中型または分散型）のいずれかをサポートしています。

- 集中型 VPN モード。デフォルト モードです。集中モードでは、VPN 接続はクラスタのマスターとのみ確立されます。

  VPN 機能を使用できるのはマスター ユニットだけであり、クラスタのハイ アベイラビリティ能力は活用されません。マスターユニットで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN 接続されたユーザにとってはサービスの中断となります。新しいマスターが選定されたときに、VPN 接続を再確立する必要があります。

  VPN トンネルをスパンド インターフェイスのアドレスに接続すると、接続が自動的にマスター ユニットに転送されます。VPN 関連のキーと証明書は、すべてのユニットに複製されます。

- 分散型 VPN モード。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散され、拡張性が提供されます。クラスタのメンバー全体に VPN 接続を分散することで、クラスタの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。

（注） 集中型 VPN クラスタリング モードは、S2S IKEv1 と S2S IKEv2 をサポートしています。

分散型 VPN クラスタリング モードは、S2S IKEv2 のみをサポートしています。

分散型 VPN クラスタリング モードは、Firepower 9300 でのみサポートされています。

リモート アクセス VPN は、集中型または分散型の VPN クラスタリング モードではサポートされていません。

ロード バランシング

ロードバランシングは、仮想クラスタ内のデバイス間でリモート アクセス VPN トラフィックを均一に分散するメカニズムです。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 コンフィギュレーションでは、2台の同一のASAが専用のフェールオーバー リンクで接続され、必要に応じて、ステートフル フェールオーバー リンク（任意）でも接続されます。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設定をサポートしています。

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

ロード バランシングの概要

リモート クライアント コンフィギュレーションで、複数の ASA を同じネットワークに接続してリモート 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 バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。これにより、システム リソースを効率的に利用でき、パフォーマンスと可用性が向上します。

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 間ネットワーク上の複数のデバイスを、論理的に仮想クラスタとしてグループ化します。

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。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、着信接続要求をバックアップ 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）。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。

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。

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、すべてのメンバーにマスターよりも 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. すべてのメンバー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. すべてのメンバー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、同じリリースまたは混在リリースの ASA から構成できます。ただし、次の制約があります。

- 同じリリースの 2 台の ASA から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 を含む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達しない可能性があります。

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 リリース 7.0(x) ソフトウェア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、このプラットフォームでは、いずれも一部のハードウェア プラットフォームにおいて、IPsec セッションの負荷とは異なる SSL VPN 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。

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。

一般的な混在クラスタ シナリオの例

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 リリース 7.1(1) ソフトウェアおよびASA リリース 7.0(x) ソフトウェアを実行しているさまざまなASA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、クラスタはさまざまなASA 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。

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、クラスタがさまざまなASA 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 バランシングについての FAQ

マルチ コンテキスト モード

Q. ロード バランシングはマルチコンテキスト モードでサポートされていますか。

A. ロード バランシングもステートフル フェールオーバーもマルチコンテキスト モードではサポートされていません。

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 メンバー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 5525-X 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 バランシングのライセンス

VPN ロード バランシングを使用するには、Security Plus ライセンスを備えた ASA モデル 5512-X、または ASA モデル 5515-X 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。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。

VPN ロード バランシングに関するガイドラインと制限事項

ロード バランシングの前提条件 （10 ページ）も参照してください。

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 モデルの ASA 5512-X（Security Plus ライセンスあり）および Model 5515-X 以降を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 Secure Mobility Client（リリース 3.0 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（IOS 831/871）
- クライアントレス SSL VPN（クライアントではない）

クライアントの考慮事項

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 を含めて、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、ロード バランシングには参加できません。

複数の ASA ノードがロードバランシングのためにクラスタ化され、AnyConnect クライアント接続にグループ URL の使用が必要な場合、個々の ASA ノードは以下を行う必要があります。

- 各リモート アクセス接続プロファイルに、各ロード バランシング仮想クラスタ アドレス（IPv4 および IPv6）のグループ URL を設定します。
- このノードの VPN ロード バランシング パブリック アドレスに対してグループ URL を設定します。

コンテキスト モード

マルチ コンテキスト モードでは、VPN ロード バランシングはサポートされません。

証明書の確認

AnyConnect でロード バランシングの証明書確認を実行し、IP アドレスによって接続がリダイレクトされている場合、クライアントにより、この IP アドレスを通してその名前チェックが

すべて実行されます。リダイレクト IP アドレスが証明書の一般名、つまり subject alt name に一覧表示されていることを確認する必要があります。IP アドレスがこれらのフィールドに存在しない場合、証明書は非信頼と見なされます。

RFC 2818 で定義されたガイドラインに従って、**subject alt name** が証明書に組み込まれている場合、名前チェックにのみ **subject alt name** を使用し、一般名は無視します。証明書を提示しているサーバの IP アドレスが証明書の **subject alt name** で定義されていることを確認します。

スタンドアロン ASA の場合、IP アドレスはその ASA の IP です。クラスタリング環境では、証明書の設定により異なります。クラスタが 1 つの証明書を使用している場合、証明書は、クラスタ IP アドレスおよびクラスタ FQDN の SAN 拡張機能を保持するほか、各 ASA の IP および FQDN を備えたサブジェクト代替名の拡張機能を含む必要があります。クラスタが複数の証明書を使用している場合、各 ASA の証明書は、クラスタ IP の SAN 拡張機能、クラスタ FQDN、個々の ASA の IP アドレスおよび FQDN を保持する必要があります。

地理的ロード バランシング

ロード バランシング環境において DNS 解決が一定の間隔で変化する場合は、存続可能時間（TTL）の値をどのように設定するかを慎重に検討する必要があります。DNS ロード バランス設定が AnyConnect との組み合わせで適切に機能するには、マッピングを処理する ASA の名前が、その ASA が選択された時点からトンネルが完全に確立されるまでの間、同じである必要があります。所定の時間が経過してもクレデンシャルが入力されない場合は、ルックアップが再び開始して別の IP アドレスが解決済みアドレスとなることがあります。DNS のマッピング先が別の ASA に変更された後でクレデンシャルが入力された場合は、VPN トンネルの確立に失敗します。

VPN の地理的ロード バランシングでは、Cisco Global Site Selector（GSS）が使用されることがあります。GSS では DNS がロード バランシングに使用され、DNS 解決の存続可能時間（TTL）のデフォルト値は 20 秒となっています。GSS での TTL の値を大きくすると、接続失敗の確率を大幅に引き下げることができます。値を大きくすると、ユーザがクレデンシャルを入力してトンネルを確立するときの認証フェーズに十分な時間を取ることができます。

クレデンシャル入力のための時間を増やすには、「起動時接続」をディセーブルにすることも検討してください。

ロード バランシングの設定

リモート クライアント コンフィギュレーションで、複数の ASA を同じネットワークに接続してリモート 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、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロード バランシングにより、システム リソースが効率的に使用され、パフォーマンスとシステム アベイラビリティが向上します。

ロード バランシングを使用するには、クラスタ内の各デバイスで以下を実行します。

- 共通の VPN ロードバランシング クラスタ属性を設定することによってロードバランシング クラスタを設定します。これには、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 共有秘密が含まれます。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。

- デバイスでロード バランシングを有効にし、パブリック アドレスとプライベート アドレスなどのデバイス固有のプロパティを定義することにより、参加するデバイスを設定します。これらの値はデバイスによって異なります。

ロード バランシングの前提条件

VPN ロード バランシングに関するガイドラインと制限事項 （8 ページ）も参照してください。

- 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）およびプライベート（内部）インターフェイスを設定しておく必要があります。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。

  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。
- 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する必要があります。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 共有秘密を確立します。
- 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。
- 暗号化を使用する場合は、インターフェイス内にロードバランシングを設定する必要があります。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。
- アクティブ/アクティブ 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。

手順

ステップ 1 VPN ロードバランシング 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。

例：

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

ステップ 2 VPN ロードバランシング 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。

例：

```
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。値の範囲は 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。

例：

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。

例：

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。

手順

ステップ 1 グローバル コンフィギュレーション モードで **vpn load-balancing** コマンドを入力して、VPN ロード バランシングを設定します。

例：

```
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から、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。

例：

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。

例：

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。

（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いて、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、指定した内部インターフェイスで **crypto ikev1 enable** コマンドを使用します。

例：

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

ステップ 5 クラスタの暗号化をイネーブルにする場合は、**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。

例：

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。

例：

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

次のタスク

複数の ASA ノードがロード バランシングのためにクラスタ化され、AnyConnect クライアント接続にグループ URL の使用が必要な場合、個々の ASA ノードで以下を行う必要があります。

- 各リモート アクセス接続プロファイルに、各ロード バランシング仮想クラスタ アドレス（IPv4 および IPv6）のグループ URL を設定します。
- このノードの VPN ロード バランシング パブリック アドレスに対してグループ URL を設定します。

tunnel-group、**general-attributes**、**group-url** コマンドを使用して、次のグループの URL を設定します。

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

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

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。

始める前に

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。

手順

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。

[**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 外部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 で DNS サーバ IP アドレスを定義します（例：dns name-server 10.2.3.4（DNS サーバの IP アドレス）。

VPN ロード バランシングの設定例

基本の VPN ロード バランシング CLI 設定

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（アクティブのみ）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# show vpn 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
```