



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 \(1 ページ\)](#)
- [VPN ロード バランシング \(3 ページ\)](#)

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 ASDM 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 接続はクラスタの制御ユニットとのみ確立されます。

VPN 機能を使用できるのは制御ユニットだけであり、クラスタの高可用性機能は活用されません。制御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。新しい制御ユニット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、接続が自動的に制御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。

VPN ロード バランシング

VPN ロードバランシングは、VPN ロードバランシンググループ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。VPN ロードバランシンググループは、2つ以上のデバイスで構成されます。1つのデバイスがディレクタとなり、その他のデバイスはメンバーデバイスとなります。グループのデバイスは、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構成を使用する必要もありません。

VPN ロードバランシンググループ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。VPN ロードバランシングにより、トラフィックはグループ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。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

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。

VPN ロード バランシング

VPN ロードバランシングについて

リモートクライアント構成で、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、VPN ロードバランシンググループを作成して、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。VPN 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。

VPN ロードバランシンググループ内のすべてのデバイスがセッションの負荷を伝送します。グループ内の1つのデバイスであるディレクタは、着信接続要求をメンバーデバイスと呼ばれる他のデバイスに転送します。ディレクタは、グループ内のすべてのデバイスを監視し、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。ディレクタの役割は、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、現在のディレクタで障害が発生すると、グループ内のメンバーデバイスの1つがその役割を引き継いで、すぐに新しいディレクタになります。

VPN ロードバランシンググループは、外部のクライアントには1つの仮想 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。これは現在のディレクタに属しています。接続の確立を試みている VPN クライアントは、最初に仮想 IP アドレスに接続します。ディレクタは、グループ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（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。VPN ロードバランシンググループのディレクタは、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。

グループ内の ASA 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 IP アドレスに再接続できます。次に、ディレクタは、グループ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。ディレクタで障害が発生した場合、グループ内のメンバーデバイスが、ただちに新しいディレクタを自動的に引き継ぎます。グループ内の複数のデバイスで障害が発生しても、グループ内のいずれかのデバイスが稼働していて使用可能である限り、ユーザはグループ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

VPN ロードバランシンググループディレクタは、IPアドレスの昇順でソートされたグループメンバーのリストを保持します。各メンバーの負荷は、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、VPNロードバランシングのSSL VPN負荷に数えられません。ディレクタは、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。すべてのメンバーがディレクタよりも1%高くなると、ディレクタはトラフィックを自身にリダイレクトします。

たとえば、1つのディレクタと2つのメンバーがある場合、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. ディレクタは、すべてのメンバーにディレクタよりも1%高い負荷がある場合、接続を使用します。
2. ディレクタが接続を使用しない場合、最も負荷率の低いメンバーがセッションを処理します。
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メンバー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アドレスが最も小さいメンバーがセッションを取得します。

VPN ロードバランシンググループ構成

VPNロードバランシンググループは、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VPNロードバランシンググループは、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VPN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VPNロードバランシンググループは、IPsecセッションおよびクライアントレスSSLセッション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。

グループのディレクタは、グループのメンバー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。

VPNロードバランシンググループで最大10のノードはテスト済みです。これより大きなグループも機能しますが、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。

VPN ロードバランシングについてよく寄せられる質問 (FAQ)

- マルチ コンテキスト モード
- IP アドレス プールの枯渇
- 固有の IP アドレス プール
- 同じデバイスでの VPN ロードバランシングとフェールオーバーの使用
- 複数のインターフェイスでの VPN ロードバランシング
- VPN ロードバランシンググループの最大同時セッション数

マルチ コンテキスト モード

- Q.** マルチコンテキストモードで VPN ロードバランシングはサポートされますか。
- A.** VPN 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 VPN 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、VPN 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。この構成では、クライアントはグループの IP アドレスに接続し、グループ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 VPN 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 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 VPN ロードバランシンググループ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で VPN ロードバランシングを使用してもパフォーマンスは向上しません。

VPN ロードバランシンググループの最大同時セッション数

- Q. それぞれ 100 ユーザの SSL VPN ライセンスを持つ 2 つの ASA 5525-X が展開されているとします。この場合、VPN ロードバランシンググループ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、グループでサポートできる最大セッション数は、グループ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。

VPN 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、VPN 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 ライセンスを検出できない場合、ASA は、VPN 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、VPN ロードバランシングシステムによる 3DES の内部構成も回避します。

VPN 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 \(7 ページ\)](#) も参照してください。

- VPN 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。VPN 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。
これを行うには、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に移動します。
- 仮想 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 IP アドレス、UDP ポート（必要に応じて）、およびグループの IPsec 共有秘密を確立します。
- グループに参加するすべてのデバイスは、IP アドレス、暗号設定、暗号キー、およびポートというクラスタ固有の同一値を共有する必要があります。
- VPN ロードバランシンググループの暗号化を使用するには、まず、内部インターフェイスを指定して **crypto ikev1 enable** コマンドを実行することで、内部インターフェイスで IKEv1 をイネーブルにする必要があります。そうしない場合、VPN ロードバランシンググループ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 ユニットもフェールオーバー用に設定されている場合は、内部および外部インターフェイスのスタンバイ IP アドレスを設定する必要があります。設定しないと、VPN ロードバランシング構成がセカンダリノードに正しく同期されず、フェールオーバー後にセカンダリユニットが VPN ロードバランシング グループに参加しません。

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

適格なクライアント

VPN 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。

- AnyConnect Secure Mobility Client (リリース 3.0 以降)
- ASA 5505 (Easy VPN クライアントとして動作している場合)
- Firepower 1010 (Easy VPN クライアントとして動作している場合)
- 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

クライアントの考慮事項

VPN 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、VPN 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、VPN 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グループ化され、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 VPN ロードバランシング仮想アドレス (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 VPN 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。VPN ロードバランシンググループ環境では、証明書の構成により異なります。グループが1つの証明書を使用している場合、証明書は、仮想 IP アドレスおよびグループ 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。グループが複数の証明書を使用している場合、各 ASA の証明書は、仮想 IP の SAN 拡張機能、グループ 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 VPN ロードバランシング

VPN 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 ロードバランシング構成が AnyConnect との組み合わせで適切に機能するには、ASA の名前からアドレスへのマッピングが、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、同じまま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。

VPN 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 VPN 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。VPN 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の可用性が向上します。

VPN ロードバランシングを使用するには、グループ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グループ属性を設定することによって、VPN ロードバランシンググループを設定します。これには、仮想 IP アドレス、UDP ポート（必要に応じて）、およびグループの IPsec 共有秘密が含まれます。グループに参加するすべてのデバイスには、グループ内でのデバイスの優先順位を除き、同一のグループ構成を設定する必要があります。
- デバイスで VPN 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。

High Availability and Scalability Wizard を使用した VPN ロード バランシングの設定

手順

- ステップ 1** [Wizards] > [High Availability and Scalability] を選択します。
- ステップ 2** [Configuration Type] 画面で、[Configure VPN Cluster Load Balancing] をクリックしてから、[Next] をクリックします。
- ステップ 3** VPN ロードバランシンググループ全体を表す 1 つの IP アドレスを選択します。グループ内のすべての 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 アドレスを指定します。
- ステップ 4** このデバイスが参加する VPN ロードバランシンググループの 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、VPN 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。
- ステップ 5** IPsec 暗号化をイネーブルにして、デバイス間で通信されるすべての VPN 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、[Enable IPsec Encryption] チェックボックスをオンにします。
- ステップ 6** IPsec 共有秘密を指定して確認します。入力した値は、連続するアスタリスク文字として表示されます。
- ステップ 7** グループ内でこのデバイスに割り当てる優先順位を指定します。値の範囲は 1 ~ 10 です。優先順位は、起動時または既存のディレクタで障害が発生したときに、このデバイスがグループディレクタになる可能性を表します。優先順位を高く設定すると（たとえば 10）、このデバイスがディレクタになる可能性が高くなります。

(注) VPN ロードバランシンググループ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、ディレクタの役割を果たすと想定されます。グループ内の各デバイスは起動するとチェックを行い、グループにディレクタがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、グループに追加されたデバイスは、グループメンバーになります。グループ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスがディレクタになります。グループ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスがディレクタになります。

- ステップ 8** [Public Interface of This Device] を選択します。
- ステップ 9** [Private Interface of This Device] を選択します。
- ステップ 10** VPN クライアント接続をデバイスにリダイレクトするとき、外部 IP アドレスの代わりにデバイスのホスト名とドメイン名を使用して、ディレクタによって完全修飾ドメイン名が送信されるようにするには、[Send FQDN to client instead of an IP address when redirecting] チェックボックスをオンにします。
- ステップ 11** [Next] をクリックします。[Summary] 画面でコンフィギュレーションを確認します。
- ステップ 12** [Finish] をクリックします。
- VPN ロードバランシンググループの構成が ASA に送信されます。

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グループ化され、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 VPN ロードバランシング仮想アドレス（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。

Group URL は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] > *connection profile name* > [Add or Edit] > [Advanced] > [Group Alias / Group URL] ペインで設定します。

VPN ロード バランシングの設定（ウィザードを使用しない場合）

手順

- ステップ 1** [Configuration] > [Remote Access VPN] > [Load Balancing] を選択します。
- ステップ 2** [Participate in Load Balancing] をオンにして、この ASA がロードバランシング クラスタに参加していることを指定します。
- ロードバランシングに参加するすべての ASA に対してこの方法でロードバランシングをイネーブルにする必要があります。
- ステップ 3** [VPN Cluster Configuration] エリアで、次のフィールドを設定します。これらの値は、仮想クラスタ全体で同じである必要があります。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。
- [Cluster IPv4 Address] : IPv4 仮想クラスタ全体を表す単一の IPv4 アドレスを指定します。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。

- **[UDP Port]** : 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。
- **[Cluster IPv6 Address]** : IPv6 仮想クラスタ全体を示す単一の IPv6 アドレスを指定します。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。IPv6 アドレスを使用したクライアントは、ASA クラスタの公開されている IPv6 アドレス経由または GSS サーバ経由で AnyConnect 接続を行うことができます。同様に、IPv6 アドレスを使用したクライアントは、ASA クラスタの公開されている IPv4 アドレス経由または GSS サーバ経由で AnyConnect VPN 接続を行うことができます。どちらのタイプの接続も ASA クラスタ内でロードバランシングできます。

(注) 少なくとも 1 台の DNS サーバに DNS サーバグループが設定されており、ASA インターフェイスの 1 つで DNS ルックアップがイネーブルにされている場合、**[Cluster IPv4 Address]** および **[Cluster IPv6 Address]** フィールドでは、仮想クラスタの完全修飾ドメイン名も指定できます。
- **[Enable IPsec Encryption]** : IPsec 暗号化をイネーブルまたはディセーブルにします。このボックスをオンにして、共有秘密情報を指定して確認します。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、このチェックボックスをオンにします。
- **[IPsec Shared Secret]** : IPsec 暗号化がイネーブルになっているときに、IPsec ピア間の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。
- **[Verify Secret]** : 共有秘密情報を再入力します。**[IPsec Shared Secret]** ボックスに入力された共有秘密情報の値を確認します。

ステップ 4 特定の ASA の [VPN Server Configuration] エリアのフィールドを設定します。

- **[Public Interface]** : このデバイスのパブリック 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。
- **[Private Interface]** : このデバイスのプライベート 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。
- **[Priority]** : クラスタ内でこのデバイスに割り当てるプライオリティを指定します。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。優先順位を高く設定すれば (10 など)、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。

(注) 仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタマスターの役割を果たすと想定されます。仮想クラスタにはマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、バックアップデバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタマスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

- [NAT Assigned IPv4 Address] : このデバイスの IP アドレスを NAT によって変換した結果の IP アドレスを指定します。NAT を使用しない場合 (またはデバイスが NAT を使用するファイアウォールの背後にはない場合) は、このフィールドを空白のままにしてください。
- [NAT Assigned IPv6 Address] : このデバイスの IP アドレスを NAT によって変換した後の IP アドレスを指定します。NAT を使用しない場合 (またはデバイスが NAT を使用するファイアウォールの背後にはない場合) は、このフィールドを空白のままにしてください。
- [Send FQDN to client] : このチェックボックスをオンにすると、VPN クラスタ マスターが VPN クライアント接続をクラスタ デバイスにリダイレクトするときに、外部 IP アドレスの代わりにクラスタデバイスのホスト名とドメイン名を使用して完全修飾ドメイン名が送信されるようになります。

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。

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。

(注) IPv6 を使用し、FQDNS をクライアントに送信するときに、これらの名前は DNS を通じて ASA で解決できる必要があります。

詳細については、「[FQDN を使用したクライアントレス SSL VPN ロード バランシングのイネーブル化 \(13 ページ\)](#)」を参照してください。

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。

Group URL は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] > *connection profile name* > [Add or Edit] > [Advanced] > [Group Alias / Group URL] ペインで設定します。

FQDN を使用したクライアントレス SSL VPN ロード バランシングのイネーブル化

手順

- ステップ 1** [Send FQDN to client instead of an IP address when redirecting] チェックボックスをオンにして、VPN ロードバランシングでの FQDN の使用をイネーブルにします。
- 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** [Configuration] > [Device Management] > [DNS] > [DNS Client] ダイアログボックスで、DNS サーバへのルートを持つインターフェイスについて、ASA での DNS ルックアップをイネーブルにします。
- ステップ 4** ASA で DNS サーバの IP アドレスを定義します。これを行うには、このダイアログボックスで [Add] をクリックします。[Add DNS Server Group] ダイアログボックスが開きます。追加する DNS サーバの IPv4 または IPv6 アドレスを入力します。たとえば、192.168.1.1 または 2001:DB8:2000::1 です。
- ステップ 5** [OK] および [Apply] をクリックします。

