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。

Cisco Secure Firewall Extensible Operating System（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接続されたユーザー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ーされて、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。

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 回めのトランザクション（ユーザーに対しては透過的）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、ユーザー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 クラスタ デバイスごとに、パブリック/外部（lbpublic）およびプライベート/内部（lbprivate）インターフェイスを設定する必要があります。

- [パブリックインターフェイス（Public interface）]：クラスタ IP アドレスへの初期通信に使用されるデバイスの外部インターフェイス。このインターフェイスは、Hello ハンドシェイクに使用されます。
- [プライベートインターフェイス（Private interface）]：ロード バランシング クラスタ メンバー間のメッセージングに使用されるデバイスの内部インターフェイス。これらのメッセージには、ロードバランシングに関連するキープアライブ、トポロジメッセージ、およびアウトオブサービス メッセージが含まれます。

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、整数のパーセンテージ（アクティブなセッションの数）として計算されます。セキュアクライアント 非アクティブセッションは、VPN ロードバランシングで SSL VPN ロードに含められません。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、セキュアクライアント、およびクライアントレス SSL VPN クライアント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 を含む VPN ロードバランシンググループは、IPsec 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は最大 10 のノードがテスト済みです。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 ディレクタの選択

ディレクタの選択プロセス

仮想クラスタ内の各非マスターは、ローカル トポロジ データベースを維持します。このデータベースは、クラスタのトポロジが変更されるたびにマスターによって更新されます。各非マスターは、マスターから Hello 応答を受信できないか、最大再試行回数に達してもマスターからキープアライブ応答を受信できない場合に、マスター選択状態になります。

メンバーは、ディレクタ選択の際に次の機能を実行します。

- ローカル トポロジ データベースで検出された各ロードバランシングユニットの優先順位を比較します。
- 同じ優先順位のユニットが 2 つ検出された場合は、下位の IP アドレスが選択されます。
- そのメンバー自体が選択された場合、選択されたメンバーは仮想 IP アドレスを要求します。
- 他のいずれかのメンバーが選択された場合、最初のメンバーは選択されたマスターに Hello 要求を送信します。
- 2 つのメンバーユニットが仮想 IP アドレスを要求しようとすると、ARP サブシステムが IP アドレスの重複状態を検出し、上位の MAC アドレスを持つメンバーにディレクタロールを辞退するように求める通知を送信します。

Hello ハンドシェイク

各メンバーは、起動時に外部インターフェイスの仮想クラスタ IP アドレスに Hello 要求を送信します。Hello 要求を受信すると、マスターは固有の Hello 要求をメンバーに送信します。ディレクタ以外のメンバーは、ディレクタからの Hello 要求を受信すると、Hello 応答を返します。これで Hello ハンドシェイクは終了になります。

Hello ハンドシェイクが完了すると、暗号化が設定されている場合、内部インターフェイスで接続が開始されます。最大再試行回数に達してもメンバーが Hello 応答を受信できない場合、メンバーはマスター選択状態になります。

キープアライブ メッセージ

メンバーとディレクタの間で Hello ハンドシェイクが完了すると、各メンバーユニットは、キープアライブ要求を負荷情報とともにマスターに定期的に送信します。ディレクタからの未処理のキープアライブ応答がない場合、通常の処理中にメンバーユニットによってキープアライブ

要求が1秒間隔で送信されます。これは、前の要求からのキープアライブ応答が受信されている限り、次のキープアライブ要求が 1 秒後に送信されることを意味します。メンバーが前のキープアライブ要求に対するディレクタからのキープアライブ応答を受信しなかった場合、1 秒後にキープアライブ要求は送信されません。代わりに、メンバーのキープアライブ タイムアウト ロジックが開始されます。

キープアライブタイムアウトは次のように機能します。

1. メンバーがディレクタからの未処理のキープアライブ応答を待っている場合、そのメンバーは通常の 1 秒間隔のキープアライブ要求を送信しません。
2. メンバーは 3 秒間待機し、4 秒後にキープアライブ要求を送信します。
3. メンバーは、ディレクタからのキープアライブ応答がない限り、上のステップ 2 を 5 回繰り返します。
4. その後、メンバーはディレクタの不在を宣言し、新しいディレクタ選択サイクルを開始します。

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

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導入するには、異なる ASA 上のセキュア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 ユーザーの SSL VPN ライセンスを持つ 2 つの Firepower 1150 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ーの最大合計数は、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 ユーザー 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のライセンス要件は次のとおりです。

- アクティブな 3DES/AES ライセンス。

  ASA は、VPN ロードバランシングを有効にする前に、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。

- ファイアウォールでアクティブ化された、この機能の有効な Security Plus ライセンス。
- 準拠するには、スマートアカウントに十分な Security Plus ライセンスが必要です。

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 （8 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無効になっています。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 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。

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。

- Secure 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、セキュアクライアント 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。

ロードバランシンググループ

- ASA は、VPN ロードバランシンググループごとに 10 台のデバイスをサポートします。
- UCAPL モードは、暗号化が無効になっている場合でも、VPN ロードバランシングをサポートしません。UCAPL モードでは、セキュアなトンネルの確立に IKEv2 を使用します。

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。

FIPS

クラスタ暗号化は FIPS ではサポートされていません。

証明書の確認

セキュアクライアント 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、クライアントによるすべての名前チェックは、この IP アドレスを通して実行されます。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ーの 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 ロードバランス構成が セキュアクライアント との組み合わせで適切に機能するには、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、ASA の名前からアドレスへのマッピングが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、ユーザー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。

IKE/IPSec セキュリティ アソシエーション

クラスタ暗号化セッションは、VPN ロードバランサトポロジのスタンバイに同期されません。

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。

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

VPN ロードバランシンググループの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 VPN 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。このコマンドは、このデバイスの VPN 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 グループ内でこのデバイスに割り当てる優先順位を設定します。値の範囲は 1 ～ 10 です。優先順位は、デバイスの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）、このデバイスがグループディレクタになる可能性が高くなります。

例：

たとえば、このデバイスにグループ内での優先順位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)#
```

VPN ロードバランシンググループ属性の設定

グループ内の各デバイスの VPN ロードバランシンググループ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グループの 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、VPN ロードバランシンググループ全体を表す単一の IP アドレスまたはFQDN を指定します。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 アドレスを選択します。IPv4 を指定する必要があります（必須）。オプションで、IPv6 アドレスを指定できます。

例：

仮想 IPv4 および IPv6 アドレスを設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster ip address 192.168.10.1 1000::2
hostname(config-load-balancing)#show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster ip address 192.168.10.1 1000::2
cluster encryption
```

VPN ロードバランシングクラスタの IPv6 アドレスを設定するには、IPv4 アドレスの設定が必須です。仮想 IPv6 アドレスのみを設定すると、エラーメッセージが表示されます。

```
hostname(config-load-balancing)#show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster encryption
participate
hostname(config-load-balancing)# cluster ip address 1000::2
ERROR: Virtual IPv4 address is not set
```

ステップ 3 グループ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、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、グループポートを 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）VPN ロードバランシンググループに対する 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、まず共有秘密を指定して検証する必要があります。 VPN ロードバランシンググループ内の 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）
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。

グループの暗号化を設定したときに IKEv1 をイネーブルにしても、グループへのデバイスの参加を設定する前にディセーブルにした場合は、**participate** コマンドを入力するとエラーメッセージが表示され、そのグループに対して暗号化はイネーブルになりません。

例：

```
hostname(config)# crypto ikev1 enable inside
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

ステップ 5 グループ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。すでに暗号化されたキーを入力する必要がある場合（たとえば、別の構成からコピーしたキー）は、**cluster key 8** *key* コマンドを入力します。

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、グループ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グループ化され、セキュアクライアント 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

デフォルトでは、ASA は VPN ロードバランシングのリダイレクトで 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、メンバーデバイスにリダイレクトされるとその証明書は無効になります。

この ASA は VPN ロードバランシング ディレクタとして、VPN クライアント接続を別のメンバーデバイス（グループ内の別の ASA）にリダイレクトするときに、DNS 逆ルックアップを使用して、そのメンバーデバイスの（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

グループ内の VPN 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 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。

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 サーバーに、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 サーバー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 サーバー IP アドレスを定義します。例：dns name-server 10.2.3.4（DNS サーバーの 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、グループのパブリック インターフェイスを **test** と指定し、グループのプライベート 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
```

VPN ロードバランシング情報の表示

VPN ロードバランシンググループのディレクタは、アクティブな セキュアクライアント 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グループ内の各 ASA からメッセージを定期的に受信します。グループ内のある ASA の容量が 100% いっぱいであると示される場合、グループディレクタ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、ユーザー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ASA 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グループディレクタに報告されません。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、グループディレクタ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 VPN 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
```

VPN ロードバランシングの機能履歴

機能名	リリース	機能情報
SAML を使用した VPN ロードバランシング	9.17(1)	ASA は、SAML 認証を使用した VPN ロードグをサポートするようになりました。
VPN ロードバランシング	7.2(1)	この機能が導入されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。