サイト間 VPN

仮想プライベート ネットワーク（VPN）は、パブリック ソース（インターネットや他のネットワーク）を使ってリモート ピア間でセキュアなトンネルを確立するネットワーク接続です。VPN は、トンネルを使用してデータ パケットを通常の IP パケット内にカプセル化し、IP ベースのネットワーク経由で転送するものです。その際、暗号化を使用してプライバシーを確保し、認証を使用してデータの整合性を確保します。

VPN の基本

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモート ユーザと企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

IPsec ベースの VPN テクノロジーは、Internet Security Association and Key Management Protocol（ISAKMP または IKE）と IPsec トンネリング標準を使用して、トンネルの構築と管理を行います。ISAKMP と IPsec は、次の処理を実行できます。

- トンネル パラメータのネゴシエーション。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネル経由のデータ転送の管理。
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理。

VPN内のデバイスは、双方向のトンネルエンドポイントとして機能します。プライベートネットワークからプレーンパケットを受信してカプセル化し、トンネルを作成して、カプセル化したパケットをトンネルのもう一方の終端に送信します。トンネルの終端では、パケットのカプセル化が解除されて最終的な宛先に送信されます。また、カプセル化されたパケットをパブリック ネットワークから受信してカプセル化を解除し、プライベート ネットワーク上の最終的な宛先に送信します。

サイト間 VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストが、セキュアな VPN トンネルを介してリモート ゲートウェイの背後にあるホストに接続します。接続は、2 つのゲートウェイの IP アドレスとホスト名、それらの背後のサブネット、2 つのゲートウェイが相互認証に使用する方式で構成されます。

Internet Key Exchange（IKE）

インターネット キー交換（IKE）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、およびセキュリティ アソシエーション（SAs）の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE ポリシーは、2 つのピア間の IKE ネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、どのセキュリティ パラメータが後続の IKE ネゴシエーションを保護するかを規定します。IKE バージョン 1（IKEv1）では、IKE ポリシーに、単一のアルゴリズムのセットと係数グループが含まれています。IKEv1 とは異なり、IKEv2 ポリシーでは、フェーズ 1 ネゴシエーション中にピアがその中から選択できるように、複数のアルゴリズムとモジュラス グループを選択できます。単一の IKE ポリシーを作成できますが、最も必要なオプションにより高い優先順位をつけるために異なるポリシーが必要となる場合もあります。サイト間 VPN では、単一の IKE ポリシーを作成できます。

IKE ポリシーを定義するには、次の内容を指定します。

- 一意の優先順位（1 ～ 65,543、1 が最高優先順位）。
- データを保護して、プライバシーを確保するための IKE ネゴシエーション用の暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証するハッシュ メッセージ 認証コード（HMAC）方式（IKEv2 では整合性アルゴリズムと呼ばれます）。
- IKEv2 では、別個の疑似乱数関数（PRF）をアルゴリズムとして使用して、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得していました。オプションは、ハッシュ アルゴリズムに使用されるものと同じです。

- 暗号キー決定アルゴリズムの強度を決定する Diffie-Hellman グループ。デバイスは、このアルゴリズムを使用して、暗号キーとハッシュ キーを導き出します。
- ピアの ID を保証するための認証方式。
- デバイスが暗号化キーを交換するまでに使用できる時間制限。

IKE ネゴシエーションが開始されると、そのネゴシエーションを開始したピアが、有効ポリシーすべてをリモート ピアに送信します。リモート ピアは所有するポリシーで一致するものを優先順位順に検索します。暗号化、ハッシュ（IKEv2 の場合、整合性と PRF）、認証、および Diffie-Hellma 値が同じで、SA ライフタイムが、送信されたポリシーのライフタイム以下の場合には、IKE ポリシー間に一致が存在します。ライフタイムが等しくない場合は、リモート ピア ポリシーから取得した短い方のライフタイムが適用されます。デフォルトでは、DES を使用した単純な IKE ポリシーが唯一の有効ポリシーです。より高い優先順位で他の IKE ポリシーを有効にして、より強力な暗号化標準をネゴシエートできますが、DES ポリシーはネゴシエーションを成功させる必要があります。

VPN 接続をセキュアにする方法

通常、VPN トンネルはインターネットなどのパブリック ネットワークを通過するため、トラフィックを保護するために接続を暗号化する必要があります。IKE ポリシーと IPsec プロポーザルの使用を適用するために、暗号化とその他のセキュリティ テクニックを定義します。

デバイス ライセンスで強力な暗号化の適用が可能な場合は、さまざまな暗号化アルゴリズム、ハッシュ アルゴリズム、Diffie-Hellman グループから選択することができます。ただし、一般的なルールとして、トンネルに適用する暗号化が強力なほど、システム パフォーマンスは低下します。効率を犠牲にすることなく十分な保護を提供するようにセキュリティとパフォーマンスのバランスを取る必要があります。

オプションの選択肢に関する特定のガイダンスを示すことはできませんが、大規模な企業や組織で運用する場合は、すでに標準が定義されていることがあります。そうでない場合は、時間をかけてオプションを検討してください。

ここでは、使用可能なオプションについて説明します。

使用する暗号化アルゴリズムの決定

IKE ポリシーまたは IPsec プロポーザルで使用する暗号化アルゴリズムを決定する場合は、選択肢が VPN 内のデバイスによってサポートされているアルゴリズムに限られます。

IKEv2 の場合は、複数の暗号化アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものの順に並べ、その順序を使用してピアとのネゴシエーションを行います。IKEv1 の場合は、1 つのオプションしか選択できません。

IPsec プロポーザルの場合、このアルゴリズムはカプセル化セキュリティ プロトコル（ESP）で使用されます。これは、認証サービス、暗号化サービス、アンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の先頭に ESP- が付けられます。

デバイス ライセンスが強力な暗号化に対応している場合は、次の暗号化アルゴリズムの中から選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

（注） 強力な暗号化の対象である場合、評価ライセンスをスマートライセンスにアップグレードする前に、暗号化アルゴリズムを確認および更新して暗号化を強化し、VPN設定が適切に機能するようにしてください。AESベースのアルゴリズムを選択します。強力な暗号化をサポートするアカウントを使用して登録されている場合、DES はサポートされません。登録後は、DES の使用対象をすべて削除するまで変更を展開できません。

- AES-GCM—（IKEv2 のみ）ガロア/カウンタ モードの Advanced Encryption Standard は、機密性とデータ発信元認証を提供するブロック暗号モードの操作であり、AES より優れたセキュリティを実現します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。GCM は NSA Suite B をサポートするために必要な AES のモードです。NSA Suite B は暗号強度に関する連邦規格を満たすためにデバイスがサポートすべき暗号化アルゴリズムのセットです。。
- AES：Advanced Encryption Standard は、DES よりも優れたセキュリティを提供し、3DES よりも効率的に計算する対称暗号アルゴリズムです。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。
- DES：56 ビットのキーを使用して暗号化するデータ暗号化規格（Data Encryption Standard）は、対称秘密キー ブロック アルゴリズムです。ライセンスアカウントが輸出規制の要件を満たしていない場合、これは唯一のオプションです。
- NULL、ESP-NULL：使用しないでください。NULL 暗号化アルゴリズムは、暗号化を使用しない認証を提供します。これは、ほとんどのプラットフォームでサポートされていません。

使用するハッシュ アルゴリズムの決定

IKE ポリシーでは、ハッシュ アルゴリズムがメッセージ ダイジェストを作成します。これは、メッセージの整合性を保証するために使用されます。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプション（整合性アルゴリズム用に 1 つと Pseudo-Random Function（PRF; 疑似乱数関数）用に 1 つ）に分かれています。

IPsec プロポーザルでは、ハッシュ アルゴリズムが、認証用のカプセル化セキュリティ プロトコル（ESP）で用されます。IKEv2 IPsec プロポーザルでは、これが整合性ハッシュと呼ばれています。IKEv1 IPsec プロポーザルでは、アルゴリズム名の先頭に ESP- が付けられ、末尾に -HMAC（「ハッシュ法認証コード」を意味する）が付けられます。

IKEv2 の場合は、複数のハッシュ アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものの順に並べ、その順序を使用してピアとのネゴシエーションを行います。IKEv1 の場合は、1 つのオプションしか選択できません。

次のハッシュ アルゴリズムから選択できます。

- [SHA (Secure Hash Algorithm)]：標準の SHA（SHA1）は、160 ビットのダイジェストを生成します。

  よりセキュアな次の SHA-2 オプションを IKEv2 設定に使用できます。NSA Suite B 暗号化仕様を実装する場合は、次のいずれかを選択します。

  - SHA256：256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
  - SHA384：384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
  - SHA512：512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。

- ヌルまたはなし（NULL、ESP-NONE）：（IPsec プロポーザルのみ）。ヌル ハッシュ アルゴリズムは、通常、テスト目的にのみ使用されます。しかし、暗号化オプションとしていずれかの AES-GCM オプションを選択した場合は、NULL 整合性アルゴリズムを選択する必要があります。ヌル以外のオプションを選択した場合でも、これらの暗号化標準では整合性ハッシュは無視されます。

使用する Diffie-Hellman 係数グループの決定

次の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec セキュリティ アソシエーション（SA）キーを生成することができます。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。両方のピアに、一致する係数グループが存在する必要があります。

AES 暗号化を選択した場合は、AES に必要な大きいキー サイズをサポートするために、Diffie-Hellman（DH）グループ 5 以上を使用する必要があります。IKEv1 ポリシーは、以下に示すすべてのグループをサポートしているわけではありません。

NSA Suite B 暗号化仕様を実装するには、IKEv2 を使用し、楕円曲線 Diffie-Hellman（ECDH）オプション（19、20、または 21）のいずれかを選択します。2048 ビット係数を使用した楕円曲線オプションとグループは、Logjam などの攻撃に耐性があります。

IKEv2 の場合は、複数のグループを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものの順に並べ、その順序を使用してピアとのネゴシエーションを行います。IKEv1 の場合は、1 つのオプションしか選択できません。

- 14：Diffie-Hellman グループ 14（2048 ビット Modular Exponential（MODP）グループ）。192 ビットのキーでは十分な保護レベルです。
- 15：Diffie-Hellman グループ 15（3072 ビット MODP グループ）。
- 16：Diffie-Hellman グループ 16（4096 ビット MODP グループ）。
- 19：Diffie-Hellman グループ 19（国立標準技術研究所（NIST）256 ビット楕円曲線モジュロプライム（ECP）グループ）。
- 20：Diffie-Hellman グループ 20（NIST 384 ビット ECP グループ）。

- 21：Diffie-Hellman グループ 21（NIST 521 ビット ECP グループ）。
- 31：Diffie-Hellman グループ 31（Curve25519 256 ビット EC グループ）。

使用する認証方式の決定

次の方法を使用して、サイト間VPN接続でピアを認証できます。

事前共有キー

事前共有キーは、接続内の各ピアで設定された秘密キー文字列です。これらのキーは、IKE が認証フェーズで使用します。IKEv1 の場合は、各ピアで同じ事前共有キーを設定する必要があります。IKEv2の場合は、各ピアに一意のキーを設定できます。

事前共有キーは、証明書に比べて拡張性がありません。多数のサイト間VPN接続を設定する必要がある場合は、事前共有キー方式ではなく証明書方式を使用します。

証明書

デジタル証明書は IKE キー管理メッセージの署名や暗号化に RSA キー ペアを使用します。サイト間 VPN 接続の両端を設定するときに、リモートピアがローカルピアを認証できるように、ローカルデバイスのアイデンティティ証明書を選択します。

証明書方式を使用するには、次の手順を実行する必要があります。

1. ローカルピアを認証局（CA）に登録し、デバイスアイデンティティ証明書を取得します。この証明書をデバイスにアップロードします。詳細については、「内部および内部 CA 証明書のアップロード」を参照してください。

   リモートピアも担当している場合、そのピアも登録してください。ピアに同じCAを使用すると便利ですが、必須ではありません。

   自己署名証明書を使用してVPN接続を確立することはできません。認証局でデバイスを登録する必要があります。

   Windows 認証局（CA）を使用してサイト間 VPN エンドポイントの証明書を作成する場合は、アプリケーションポリシー拡張にIPセキュリティエンドシステムを指定する証明書を使用する必要があります。これは(Windows CAサーバ)の[拡張]タブにある証明書の[プロパティ]ダイアログボックスで確認できます。この拡張のデフォルトは IP セキュリティ IKE 中間であり、Device Manager を使用して設定されたサイト間 VPN では機能しません。

2. ローカル ピアのアイデンティティ証明書に署名するために使用された、信頼できる CA 証明書をアップロードします。中間CAを使用した場合は、ルート証明書と中間証明書を含む完全なチェーンをアップロードします。詳細については、「信頼できる CA 証明書のアップロード」を参照してください。

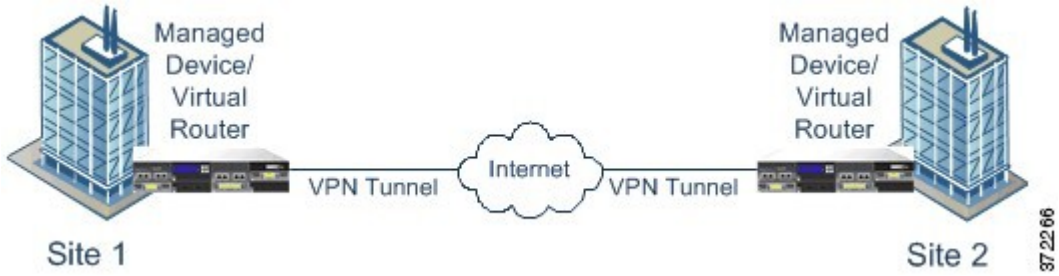
3. リモートピアが異なる CA で登録されていた場合、リモートピアのアイデンティティ証明書に署名するために使用した信頼できるCA証明書もアップロードします。リモートピアを制御する組織から証明書を取得します。中間CAを使用した場合は、ルート証明書と中間証明書を含む完全なチェーンをアップロードします。

4. サイト間VPN接続を設定したら、証明書方式を選択し、ローカルピアのアイデンティティ証明書を選択します。接続の両端が、接続のローカルエンドの証明書を指定します。リモート ピアの証明書は指定しません。

VPN トポロジ

Device Manager を使用して設定できるのは、ポイントツーポイント VPN 接続のみです。すべての接続はポイントツーポイントですが、デバイスが参加する各トンネルを定義することで、より大規模なハブアンドスポーク VPN、またはメッシュ VPN にリンクできます。

次の図に、一般的なポイントツーポイント VPN トポロジを示します。ポイントツーポイント VPN トポロジでは、2 つのエンドポイントが相互に直接通信します。2 つのエンドポイントをピア デバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。



動的にアドレス指定されたピアによるサイト間 VPN 接続の確立

ピアの IP アドレスが不明な場合でも、ピアへのサイト間 VPN 接続を作成できます。これは、次のような場合に役立ちます。

- ピアが DHCP を使用してそのアドレスを取得した場合は、特定の静的 IP アドレスを持つリモートエンドポイントに依存することはできません。
- 不特定多数のリモートピアが、ハブアンドスポークトポロジのハブとして機能するデバイスとの接続を確立できるようにする場合。

動的にアドレス指定されたピアBへのセキュアな接続を確立する必要がある場合は、接続の終了 A にスタティック IP アドレスがあることを確認する必要があります。次に、A で接続を作成するときに、ピアのアドレスがダイナミックであることを指定します。ただし、ピアBで接続を設定する際は、リモートピアアドレスとして A の IP アドレスを入力します。

システムがサイト間 VPN 接続を確立する場合、ピアがダイナミックアドレスを持つすべての接続は応答のみとなります。つまり、リモートピアは接続を開始するものである必要があります。リモートピアが接続を確立しようとすると、デバイスは事前共有キーまたは証明書（接続で定義されているいずれかの方式）を使用して接続を検証します。

VPN 接続はリモートピアが接続を開始した後にのみ確立されるため、VPN トンネルのトラフィックを許可するアクセス制御ルールに一致するすべての発信トラフィックは、接続が確立

されるまでドロップされます。これにより、適切な暗号化と VPN 保護のないデータがネットワークから流出しないようになります。

仮想トンネルインターフェイスとルートベースの VPN

従来は、VPN トンネルを介して暗号化される特定のローカルネットワークとリモートネットワークを定義することにより、サイト間 VPN 接続を設定していました。これらは、VPN 接続プロファイルの一部である暗号マップで定義されます。このタイプのサイト間 VPN は、ポリシーベースと呼ばれます。

また、ルートベースのサイト間 VPN を設定することもできます。この場合は、仮想トンネルインターフェイス（VTI）を作成します。これは、特定の物理インターフェイス（通常、外部インターフェイス）に関連付けられた仮想インターフェイスです。その後、ルーティングテーブルと静的ルートおよび動的ルートを使用して、目的のトラフィックを VTI に転送します。VTI（出力）を介してルーティングされるトラフィックは、VTI 用に設定した VPN トンネルを介して暗号化されます。

そのため、ルートベースのサイト間 VPN を使用すると、VPN 接続プロファイルを一切変更することなく、ルーティングテーブルを変更するだけで、特定の VPN 接続で保護されたネットワークを管理できます。リモートネットワークの追跡を継続し、前述の変更に対応して VPN 接続プロファイルを更新する必要はありません。その結果、クラウド サービス プロバイダーや大企業の VPN 管理が簡素化されます。

さらに、VTI のアクセス制御ルールを作成して、トンネルで許可されるトラフィックのタイプを微調整できます。たとえば、侵入検査や、URL およびアプリケーションフィルタリングを適用できます。

ルートベースの VPN を設定するためのプロセスの概要

概要として、ルートベースのサイト間 VPN をセットアップするプロセスには、次の手順が含まれます。

手順

ステップ 1 ローカルエンドポイントの IKEv1/2 ポリシーと IPsec プロポーザルを作成します。

ステップ 2 リモートピアに面する物理インターフェイスに関連付けられた仮想トンネルインターフェイス（VTI）を作成します。

ステップ 3 VTI、IKE ポリシー、および IPsec プロポーザルを使用するサイト間 VPN 接続プロファイルを作成します。

ステップ 4 リモートピア（およびリモート VTI）に同じ IKE および IPsec プロポーザルを作成し、このローカル VTI をリモートエンドポイントとして指定（リモートピアの観点から）するサイト間 VPN 接続プロファイルを作成します。

ステップ 5 トンネルを介して適切なトラフィックを送信するために、両方のピアでルートとアクセス制御ルールを作成します。

両方向のトラフィックフローを可能にするために、各エンドポイントのルートとアクセス制御が相互にミラーリングされていることを確認してください。

静的ルートには、次のような一般的特性があります。

- [インターフェイス（Interface）]：仮想トンネルインターフェイス（VTI）の名前。
- [ネットワーク（Networks）]：リモートエンドポイントによって保護されるリモートネットワークを定義するネットワークオブジェクト。
- [ゲートウェイ（Gateway）]：VPN トンネルのリモートエンドポイントの IP アドレスを定義するネットワークオブジェクト。

仮想トンネルインターフェイスとルートベースの VPN に関するガイドライン

IPv6 のガイドライン

仮想トンネルインターフェイスは IPv4 アドレスのみをサポートしています。VTI で IPv6 アドレスを設定することはできません。

追加のガイドライン

- 最大1024個のVTIを作成できます。
- VTI ルートベース VPN では、リバース ルート インジェクション（静的または動的）を設定できません（リバース ルート インジェクションは Threat Defense API のみを使用して設定可能）。
- VTIをローカルインターフェイスとして選択する場合は、動的ピアアドレスを設定できません。
- VTIをローカルインターフェイスとして選択する場合は、リモートバックアップピアを設定できません。
- カスタム仮想ルータに割り当てられている送信元インターフェイスにVTIを作成することはできません。仮想ルータを使用する場合、グローバル仮想ルータのインターフェイスのみで、VTIを設定できます。
- IKE および IPsec のセキュリティ アソシエーションには、トンネル内のデータ トラフィックに関係なく、継続的にキーの再生成が行われます。これにより、VTI トンネルは常にアップした状態になります。
- ルートベースの接続プロファイルで IKEv1 と IKEv2 の両方を設定することはできません。1 つのバージョンの IKE のみを設定する必要があります。
- 暗号マップに設定されるピアアドレスと VTI のトンネル宛先が異なる場合は、同じ物理インターフェイスで異なる VTI およびポリシーベース（暗号マップ）設定を指定できます。
- VTI を介してサポートされるのは BGP ルーティングプロトコルだけです。

- システムが IOS IKEv2 VTI クライアントを終端している場合は、IOS VTI クライアントによって開始されたセッションのモード CFG 属性をシステムが取得できないため、IOS での設定交換要求を無効にします。
- ルートベースのサイト間 VPN は双方向として設定されます。つまり、VPN トンネルのどちらのエンドポイントでも接続を開始できます。接続プロファイルを作成したら、このエンドポイントを唯一のイニシエータ（INITIATE_ONLY）に変更するか排他的にレスポンダ（RESPOND_ONLY）に変更することができます。必ず、補完的な接続タイプを使用するようにリモートエンドポイントを変更してください。この変更を行うには、API エクスプローラに移動し、GET /devices/default/s2sconnectionprofiles を使用して接続プロファイルを見つける必要があります。その後、本文の内容をコピーして PUT /devices/default/s2sconnectionprofiles/{objId} メソッドに貼り付け、[connectionType] を更新して目的のタイプを指定して、メソッドを実行します。

IPsec フローのオフロード

IPsec フローのオフロードを使用するように、サポートするデバイスモデルを設定できます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。Cisco Secure Firewall 1200 シリーズでは、デバイスのパフォーマンスを向上させるために、IPsec 接続が Marvell Cryptographic Accelerator（CPT）にオフロードされます。

オフロード操作は、特に、入力の事前復号および復号処理と出力の事前暗号化および暗号化処理に関連しています。システムソフトウェアは、セキュリティポリシーを適用するための内部フローを処理します。

IPsec フローのオフロードはデフォルトで有効になっており、次のデバイスタイプに適用されます。

- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100

IPsec フローのオフロードに関する制約事項

次の IPsec フローはオフロードされません。

- IKEv1 トンネル。IKEv2 トンネルのみがオフロードされます。IKEv2 は、より強力な暗号をサポートしています。
- ボリュームベースのキー再生成が設定されているフロー。
- 圧縮が設定されているフロー。
- トランスポートモードのフロー。トンネルモードのフローのみがオフロードされます。
- AH 形式。ESP/NAT-T 形式のみがサポートされます。
- ポストフラグメンテーションが設定されているフロー。

- 64 ビット以外のアンチリプレイ ウィンドウ サイズを持ち、アンチリプレイが無効になっていないフロー。
- ファイアウォールフィルタが有効になっているフロー。

IPsec フローのオフロードの設定

IPsec フローのオフロードは、この機能をサポートするハードウェア プラットフォームではデフォルトで有効になっています。設定を変更するには、FlexConfig を使用して **flow-offload-ipsec** コマンドを実装します。このコマンドの詳細については、ASA コマンドリファレンスを参照してください。

サイト間 VPN の管理

仮想プライベート ネットワーク（VPN）は、パブリック ソース（インターネットや他のネットワーク）を使ってリモートピア間でセキュアなトンネルを確立するネットワーク接続です。VPN は、トンネルを使用してデータ パケットを通常の IP パケット内にカプセル化し、IP ベースのネットワーク経由で転送するものです。その際、暗号化を使用してプライバシーを確保し、認証を使用してデータの整合性を確保します。

ピア デバイスへの VPN 接続を作成することができます。すべての接続はポイントツーポイントですが、すべての関連接続を設定することによって、デバイスをより大きなハブアンドスポークまたはメッシュ VPN にリンクできます。

始める前に

次の事実によって、再作成できるサイト間 VPN 接続のタイプと数が制御されます。

- VPN 接続は暗号化を使用して、ネットワークのプライバシーを確保します。使用できる暗号化アルゴリズムは、基本ライセンスで強力な暗号化が許可されているかどうかによって異なります。これは、Cisco Smart License Manager に登録する際にデバイス上でエクスポート制御機能を許可するオプションを選択したかどうかによって制御されます。評価ライセンスを使用している場合または輸出規制機能を有効にしていない場合は、強力な暗号化を使用できません。
- 最大 20 の一意の IPsec プロファイルを作成できます。一意性は、IKEv1/v2 プロポーザルと証明書、接続タイプ、DH グループ、および SA ライフタイムの組み合わせによって決定されます。既存のプロファイルを再利用できます。そのため、すべてのサイト間 VPN 接続に同じ設定を使用すると、1 つの一意の IPsec プロファイルを持つことになります。一意の IPsec プロファイルの数が上限の 20 に達すると、既存の接続プロファイルに使用したものと同じ属性の組み合わせを使用しないかぎり、新しいサイト間 VPN 接続を作成できません。

手順

ステップ 1 [デバイス（Device）] をクリックし、次に [サイト間VPN（Site-to-Site VPN）] グループの [設定の表示（View Configuration）] をクリックします。

これで、[サイト間VPN（Site-to-Site VPN）] ページが開き、設定済みのすべての接続が表示されます。

ステップ 2 次のいずれかを実行します。

- 新しいサイト間 VPN 接続を作成する場合は、[+] ボタンをクリックします。サイト間 VPN 接続の設定 （12 ページ）を参照してください。

  既存の接続がなければ、[サイト間接続の作成（Create Site-to-Site Connection）] ボタンをクリックすることもできます。

- 既存の接続を編集するには、その接続の編集（）アイコンをクリックします。サイト間 VPN 接続の設定 （12 ページ）を参照してください。
- 接続設定のサマリーをクリップボードにコピーするには、その接続の [コピー（copy）] アイコン（）をクリックします。この情報をドキュメントに貼り付け、そのドキュメントを管理者に送信することで、リモート デバイスの接続設定に利用できます。
- 不要な接続を削除するには、その接続の削除アイコン（）をクリックします。

サイト間 VPN 接続の設定

ポイントツーポイント VPN 接続を作成することで、デバイスを別のデバイスにリンクできます。ただし、リモートデバイス所有者の協力と許可を得ることが前提となります。すべての接続はポイントツーポイントですが、デバイスが参加するトンネルそれぞれを定義することで、ハブアンドスポークまたはメッシュ構造の大規模な VPN にリンクすることができます。

始める前に

ローカル ネットワークとリモート ネットワークの組み合わせごとに作成できる VPN 接続は 1 つに限られます。ただし、リモート ネットワークがそれぞれの接続プロファイル内で固有であれば、ローカル ネットワークに対して複数の接続を作成できます。

リモートネットワークが重複している場合は、より制限の厳しい接続プロファイルを最初に作成するように注意してください。システムはトンネルを、表示される順序（アルファベット順）ではなく、接続プロファイルを作成した順序で作成します。

たとえば、リモートエンドポイント A へのアクセスには 192.16.0.0/16 から 10.91.0.0/16 までをトンネリングさせ、192.16.0.0/24 から 10.0.0.0/8 の残りへのトンネリングはリモートエンドポ

イント B を介して行う場合、B の接続プロファイルを作成する前に A の接続プロファイルを作成する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、次に [サイト間VPN（Site-to-Site VPN）] グループの [設定の表示（View Configuration）] をクリックします。

ステップ 2 次のいずれかを実行します。

- 新しいサイト間 VPN 接続を作成する場合は、[+] ボタンをクリックします。

  既存の接続がなければ、[サイト間接続の作成（Create Site-to-Site Connection）] ボタンをクリックすることもできます。

- 既存の接続を編集する場合は、対象の接続の編集アイコン（  ）をクリックします。

不要な接続を削除するには、その接続の削除アイコン（  ）をクリックします。

ステップ 3 ポイントツーポイント VPN 接続のエンドポイントを定義します。

- [接続プロファイル名（Connection Profile Name）]：接続の名前を最大 64 文字で、スペースを含めずに入力します。たとえば、「MainOffice」と入力します。IP アドレスを名前として使用することはできません。
- [タイプ（Type）]：VPN トンネルを介して送信する必要があるトラフィックを識別する方法。次のいずれかを選択します。
  - [ルートベース（VTI）（Route Based (VTI)）]：ルーティングテーブル（主に静的ルート）を使用して、トンネルに参加するローカルネットワークとリモートネットワークを定義します。このオプションを選択する場合は、仮想トンネルインターフェイス（VTI）をローカル VPN アクセスインターフェイスとして選択する必要があります。また、トンネルのリモートエンドには静的 IP アドレスを使用する必要があります。VPN 接続プロファイルを作成した後に、必ず、VTI の適切な静的ルートとアクセス制御ルールを設定してください。
  - [ポリシーベース（Policy Based）]：ローカルネットワークとリモートネットワークを、サイト間 VPN 接続プロファイルで直接指定します。これは、VPN トンネルによって保護する必要があるトラフィックを定義するための従来のアプローチです。
- [ローカルサイト（Local Site）]：以下のオプションによってローカルエンドポイントを定義します。
  - [ローカル VPN アクセス インターフェイス（Local VPN Access Interface）]：リモートピアに接続を許可するインターフェイスを選択します。通常は、外部インターフェイスを選択します。ブリッジグループのメンバーとなっているインターフェイスを選択することはできません。ポリシーベースの接続のバックアップピアを設定する場合は、ピアが接続できるすべてのインターフェイスを選択してください。ルートベースの接続の場合、選択できるインターフェイスは 1 つだけです。

- [ローカルネットワーク（Local Network）]：（ポリシーベースのみ）[+] をクリックし、VPN接続に参加する必要があるローカルネットワークを識別するネットワークオブジェクトを選択します。選択したネットワークのユーザが、この接続を介してリモート ネットワークに到達できるようになります。

（注）
これらのネットワークには IPv4 または IPv6 アドレスを使用できますが、接続の両側に一致するアドレス タイプがなければなりません。たとえば、ローカル IPv4 ネットワークの VPN 接続には、少なくとも 1 つのリモート IPv4 ネットワークが必要です。単一の接続の両側で IPv4 と IPv6 を組み合わせることはできます。エンドポイントの保護対象ネットワークを重複させることはできません。

- [リモートサイト（Remote Site）]：これらのオプションでリモート エンドポイントを定義します。
  - [スタティック（Static）]/[ダイナミック（Dynamic）]：リモートピアの IP アドレスが静的または動的（DHCP などを使用して）のどちらで定義されるか。[スタティック（Static）] を選択した場合、リモートピアの IP アドレスも入力します。[ダイナミック（Dynamic）] を選択した場合、リモート ピアのみがこの VPN 接続を開始できるようになります。

    ルートベースの VPNの場合は、選択できるのは [スタティック（Static）] のみです。
  - [リモートIPアドレス（Remote IP Address）]（スタティック アドレス指定のみ）：VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレスを入力します。
  - [リモートバックアップピア（Remote Backup Peers）]：（オプション、ポリシーベースの接続のみ）[ピアの追加（Add Peer）] をクリックして、リモートエンドポイントのバックアップを追加します。プライマリエンドポイントが使用できなくなると、システムはバックアップピアの 1 つで VPN 接続を再確立しようとします。複数のバックアップを追加できます。

    各バックアップピアを設定するときに、そのピアで使用する事前共有キーと証明書を設定できます。プライマリリモートピアの設定に使用したのと同じ手法を使用します。接続プロファイルに設定されている同じ値を使用するには、これらの設定を空白のままにします。

    最初のバックアップピアを設定後、[別のピアを追加（Add Another Peer）] をクリックして別のピアを追加するか、ピアを削除するか、または [編集（Edit）] をクリックしてピアの設定を変更できます。

    バックアップピアがプライマリピアとは異なるインターフェイスを介して到達可能な場合は、[ローカルVPNアクセスインターフェイス（Local VPN Access Interface）] で必要なインターフェイスを選択していることを確認します。
  - [リモートネットワーク（Remote Network）]：（ポリシーベースのみ）[+] をクリックし、VPN接続に参加する必要があるリモートネットワークを識別するネットワークオ

ブジェクトを選択します。選択したネットワークのユーザが、この接続を介してローカル ネットワークに到達できるようになります。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 VPN のプライバシー設定を定義します。

（注）
使用しているライセンスにより、選択できる暗号化プロトコルが決まります。最も基本的なオプション以外の強力な暗号化、つまりエクスポート制御の必要を満たす暗号化を選択する資格がなければなりません。

- [IKE バージョン 2（IKE Version 2）]、[IKE バージョン 1（IKE Version 1）]：インターネット キー エクスチェンジ（IKE）ネゴシエーションで使用する IKE バージョンを選択します。ポリシーベースの接続の場合は、いずれかまたは両方を選択できます。ルートベースの場合、選択できるのは一方のみです。もう一方のピアとの接続のネゴシエーションを試行する際、デバイスはユーザが許可したバージョンの内もう一方のピアが受け入れるバージョンを使用します。両方のバージョンを許可すると、最初に選択したバージョンでのネゴシエーションが正常に行われなかった場合、デバイスはもう一方のバージョンに自動的にフォールバックします。IKEv2 が設定されている場合、最初に試行されるのは常に IKEv2 です。ネゴシエーションで使用するには、両方のピアが IKEv2 をサポートする必要があります。

- [IKE ポリシー（IKE Policy）]：インターネット キー エクスチェンジ（IKE）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、IPsec セキュリティ アソシエーション（SA）の自動的な確立に使用されるキー管理プロトコルです。これはグローバル ポリシーであり、有効にするオブジェクトがすべての VPN に適用されます。IKE バージョンごとに現在グローバルに有効にされているポリシーを確認する場合や、新しいポリシーを有効にして作成する場合は、[編集（Edit）] をクリックします。詳細については、グローバル IKE ポリシーの設定 （19 ページ）を参照してください。

- [IPsec プロポーザル（IPsec Proposal）]：IPsec プロポーザルは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルおよびアルゴリズムの組み合わせを定義します。[編集（Edit）] をクリックし、IKE バージョンごとにプロポーザルを選択します。許可するプロポーザルをすべて選択します。システムのデフォルト値をそのまま選択する場合は、[デフォルトに設定（Set Default）] をクリックします。デフォルト値は、該当するエクスポート コンプライアンスによって異なります。システムはピアと合意に至るまで、最も強力なプロポーザルから弱いものへの順でネゴシエートします。詳細については、「IPsec プロポーザルの設定 （25 ページ）」を参照してください。

- [認証タイプ（Authentication Type）]：VPN 接続でピアを認証する方法（[事前共有手動キー（Preshared Manual Key）] または [証明書（Certificate）] のいずれか）。また、選択内容に基づいて次のフィールドに入力する必要があります。IKEv1 の場合、接続用に設定された IKEv1 ポリシーオブジェクトで選択された認証方式と選択内容が一致する必要があります。オプションの詳細については、使用する認証方式の決定 （6 ページ）を参照してください。

- （IKEv2）[ローカル事前共有キー（Local Preshared Key）]、[リモートピア事前共有キー（Remote Peer Preshared Key）]：VPN 接続のためにこのデバイスとリモート デバイスで定義されたキー。IKEv2 では異なるキーを使用できます。キーは 1 ～ 127 文字の英数字で指定できます。
- （IKEv1）[事前共有キー（Preshared Key）]：ローカル デバイスとリモート デバイスの両方で定義されているキー。キーは 1 ～ 127 文字の英数字で指定できます。
- [証明書（Certificate）]：ローカル ピアのデバイス アイデンティティ証明書。これは、認証局(CA)から取得した証明書である必要があります。自己署名証明書は使用できません。証明書をアップロードしていない場合は、[新しいオブジェクトの作成]リンクをクリックします。また、アイデンティティ証明書の署名に使用されたルート CA 証明書および信頼できる中間 CA 証明書をアップロードする必要があります。アップロードされた証明書の [検証の使用（Validation Usage）] が [IPsecクライアント（IPsec Client）]を含むように設定されていることを確認します。まだアップロードしていない場合は、このウィザードを閉じた後に実行できます。

- [IPsec設定]: セキュリティ アソシエーションのライフタイム。ライフタイムに達すると、システムはセキュリティアソシエーションを再ネゴシエートします。システムは、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティアソシエーションのライフタイムとして使用します。ライフタイムには、"指定時刻" ライフタイムと "トラフィック量" ライフタイムの2つがあります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。
  - [ライフタイム期間]: セキュリティ アソシエーションの有効期限が切れるまでの存続時間(秒数)を指定します。指定できる範囲は 120 ～ 214783647 秒です。グローバルのデフォルトは 28,800 秒（8 時間）です。
  - [ライフタイムサイズ]: 所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティアソシエーションを使用してピア間を通過できるトラフィックの量をKB単位で指定します。範囲は10ー2147483647 KB、または空白です。グローバルなデフォルトは4,608,000 KBです。サイズベースの制限を削除し、期間を唯一の制限として使用するには、フィールドを空白のままにします。

- [NAT免除（NAT Exempt）]：（ポリシーベースのみ）ローカル VPN アクセスインターフェイスで VPN トラフィックを NAT ポリシーから免除するかどうか。NAT ルールをローカル ネットワークに適用しない場合は、そのローカル ネットワークをホストしているインターフェイスを選択します。このオプションは、ローカル ネットワークが（ブリッジ グループ メンバーではなく）単一のルーテッド インターフェイスの背後にある場合にのみ機能します。ローカル ネットワークが複数のルーテッド インターフェイスの背後にある場合、または 1 つ以上のブリッジ グループ メンバーになっている場合は、手動で NAT 免除ルールを作成する必要があります。必要なルールを手動で作成する方法については、NAT からのサイト間 VPN トラフィックの免除 （31 ページ）を参照してください。
- [Perfect Forward Secrecy 用 Diffie-Hellman グループ（Diffie-Helman Group for Perfect Forward Secrecy）]：暗号化された交換ごとに一意のセッション キーを生成および使用するために

Perfect Forward Secrecy（PFS）を使用するかどうかを指定します。一意のセッション キーを使用することによって、以降の復号から交換が保護されます。このことは、交換全体が記録され、攻撃者がエンドポイントデバイスで使用される事前共有キーまたは秘密キーを入手している場合であっても該当します。Perfect Forward Secrecy を有効にするには、[モジュラス グループ（Modulus Group）] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムを選択します。IKEv1 と IKEv2 の両方を有効にする場合、オプションはIKEv1 でサポートされるものに制限されます。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （5 ページ）を参照してください。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 概要を確認してから [完了（Finish）] をクリックします。

概要情報はクリップボードにコピーされます。この情報はドキュメントに貼り付けて、リモート ピアの設定、またはピアの設定責任者に送信するために使用できます。

サイト間 VPN 経由のトラフィックの許可 （18 ページ）で説明したように、追加の手順で VPN トンネル内のトラフィックを許可する必要があります。

設定を展開後、デバイスCLIにログインし、**show ipsec sa**コマンドを使用してエンドポイントでセキュリティ アソシエーションが確立されることを確認します。「サイト間 VPN 接続の確認 （28 ページ）」を参照してください。

仮想トンネルインターフェイスの設定

ルートベースのサイト間VPN接続プロファイルでのみ仮想トンネルインターフェイス（VTI）を使用できます。VTIは物理インターフェイスに関連付けられており、これを介してリモートピアへの VPN 接続が確立されます。仮想インターフェイスを使用すると、サイト間 VPN 接続が簡素化され、接続プロファイルで VPN のローカルネットワークとリモートネットワークを指定するのではなく、静的ルートと動的ルートを使用してトラフィックを制御できます。

手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーのリンクをクリックして、[仮想トンネルインターフェイス（Virtual Tunnel Interfaces）] をクリックします。

ステップ 2 次のいずれかを実行します。

- [+] または [仮想トンネルインターフェイスの作成（Create Virtual Tunnel Interface）] をクリックして新しいインターフェイスを作成します。
- 既存のインターフェイスの編集アイコン（  ）をクリックします。

インターフェイスが不要になった場合は、そのインターフェイスの削除アイコン（）をクリックします。インターフェイスを削除する前に、まず、そのインターフェイスを使用するサイト間接続プロファイルをすべて削除する必要があります。

ステップ 3 次のオプションを設定します。

- [名前（Name）]：インターフェイス名（最大 48 文字）。既存のインターフェイスの名前を変更すると、それを含むすべてのポリシーとオブジェクトでも名前が自動的に変更されます。名前に大文字を使用することはできません。
- [ステータス（Status）]：スライダをクリックして有効の位置にします（）。
- [Description]：（任意） 説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。
- [トンネル ID（Tunnel ID）]：0 ー 10413 の番号。この番号が「Tunnel」という語に付加されて、インターフェイスのハードウェア名が形成されます。まだ別の VTI に使用されていない番号を選択する必要があります。たとえば、インターフェイス Tunnel1 を作成するには 1 を入力します。
- [トンネルの送信元（Tunnel Source）]：この VTI に関連付けられるインターフェイスを選択します。トンネルの送信元は、仮想トンネルインターフェイスで定義されたサイト間 VPN がリモートエンドポイントに接続するためのインターフェイスです。外部インターフェイスなどのリモートエンドポイントに到達できるインターフェイスを選択します。送信元インターフェイスには、名前付きの物理インターフェイス、サブインターフェイス、または Etherchannel を指定できます。インターフェイスをブリッジ仮想インターフェイス（BVI）のメンバーにすることはできません。
- [IPアドレスとサブネットマスク（IP Address and Subnet Mask）]：IPv4 アドレスおよび関連サブネットマスク。たとえば、192.168.1.1/24 または /255.255.255.0 です。このアドレスは、トンネル送信元インターフェイスのアドレスと同じサブネット上にある必要はありません。ただし、送信元インターフェイスでリモートアクセス(RA)VPNを設定する場合、VTI IPアドレスはRA VPNに設定されたアドレスプール内にはありません。

ステップ 4 **[OK]** をクリックします。

サイト間 VPN 経由のトラフィックの許可

サイト間 VPN トンネル内のトラフィックフローを有効にするには、次の方法のいずれかを使用します。

- **sysopt connection permit-vpn** コマンドを設定します。これにより、VPN 接続と一致するトラフィックがアクセス コントロール ポリシーから免除されます。このコマンドのデフォルトは **no sysopt connection permit-vpn** で、VPN トラフィックをアクセス コントロール ポリシーでも許可する必要があることを意味します。

これはVPNでトラフィックを許可する一層安全なメソッドです。外部ユーザが保護されたリモートネットワーク内のIPアドレスをスプーフィングできないためです。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

このコマンドを設定するのに適した方法は、リモート アクセス VPN 接続プロファイルを作成し、そこで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（Bypass Access Control policy for decrypted traffic）] オプションを選択することです。RA VPN を設定したくない場合、または RA VPN を設定できない場合、FlexConfig を使用してコマンドを設定することができます。

（注） この方式は、仮想トンネルインターフェイス（VTI）で設定されたルートベースの VPN 接続には適用されません。ルートベースの VPN のアクセス制御ルールは常に設定する必要があります。

- リモート ネットウェアからの接続を許可するアクセス制御ルールを作成します。この方法では、VPN トラフィックが検査され、高度なサービスを接続に適用できることが保証されます。欠点は、外部ユーザが IP アドレスになりすまして内部ネットワークにアクセスする可能性があることです。

グローバル IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット キー交換）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKE ポリシー オブジェクトは、これらのネゴシエーション用の IKE プロポーザルを定義します。有効化されたオブジェクトは、ピアが VPN 接続をネゴシエートする際に使用されます。接続ごとに異なる IKE ポリシーを指定することはできません。各オブジェクトの相対的な優先順位に従って、最初に試行されるポリシーが決まります。番号が小さいほど優先順位が高くなります。両方のピアがサポートするポリシーをネゴシエーションで見つけられない場合、接続は確立されません。

グローバル IKE ポリシーを定義するには、それぞれの IKE バージョンに関して有効にするオブジェクトを選択します。事前定義済みのオブジェクトが独自の要件を満たさない場合は、新しいポリシーを作成してセキュリティ ポリシーを実施できます。

次の手順では、[オブジェクト（Objects）]ページでグローバルポリシーを設定する方法について説明します。また、IKE ポリシー設定の [編集（Edit）] をクリックすることにより、VPN 接続を編集する際にポリシーを有効化、無効化、および作成することもできます。

（注） 最大20のIKEポリシーを有効にできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [IKE ポリシー（IKE Policies）] を選択します。

IKEv1 のポリシーと IKEv2 のポリシーは別個のリストに表示されます。

ステップ 2 それぞれの IKE バージョンに関して許可する IKE ポリシーを有効化します。

a) オブジェクト テーブルの上の [IKEv1] または [IKEv2] を選択すると、そのバージョンのポリシーが表示されます。

b) [状態（State）] トグルをクリックして、適切なオブジェクトを有効化し、要件に適合しないオブジェクトを無効化します。

セキュリティ要件の一部が既存のオブジェクトに反映されていない場合は、新しいオブジェクトを定義して必要な要件を実装できます。詳細については、次のトピックを参照してください。

- IKEv1 ポリシーの設定 （21 ページ）
- IKEv2 ポリシーの設定 （22 ページ）

c) 相対的な優先順位が要件に一致することを確認します。

ポリシーの優先順位を変更する必要がある場合は、編集します。事前定義されたシステムポリシーの場合、優先順位を変更するには、そのポリシーの独自のバージョンを作成する必要があります。

優先順位は相対的であり、絶対的ではありません。たとえば、優先順位 80 は 160 より高くなります。有効にしたオブジェクトの中で 80 が最も優先順位の高いオブジェクトであれば、そのオブジェクトが最初に選択されるポリシーになります。その後、優先順位 25 のポリシーを有効にすると、そのオブジェクトが最初に選択されるポリシーになります。

d) 両方の IKE バージョンを使用する場合は、もう一方のバージョンでこのプロセスを繰り返します。

IKEv1 ポリシーの設定

Internet Key Exchange（IKE; インターネットキーエクスチェンジ）バージョン 1 ポリシー オブジェクトには、VPN 接続を定義する際に IKEv1 ポリシーで必要となるパラメータが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動確立に使用されます。

事前定義済みの IKEv1 ポリシーがいくつか用意されています。ニーズに適したものがあれば、単に [状態（State）] トグルをクリックしてそれらを有効化します。または新しいポリシーを作成して、他のセキュリティ設定の組み合わせを実装することもできます。システム定義されたオブジェクトを編集/削除することはできません。

次の手順では、[オブジェクト（Objects）] ページからオブジェクトを直接作成および編集する方法を説明します。また、オブジェクトの一覧に表示される [新しい IKE ポリシーの作成（Create New IKE Policy）] リンクをクリックすることにより、VPN 接続の IKEv1 設定を編集する際に IKEv1 ポリシー オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [IKE ポリシー（IKE Policies）] を選択します。

ステップ 2 オブジェクト テーブルの上の [IKEv1] を選択し、IKEv1 ポリシーを表示します。

ステップ 3 システム定義されたポリシーの中に要件に合うポリシーがあれば、[状態（State）] トグルをクリックしてそれらを有効化します。

不要なポリシーを無効化する場合にも、[状態（State）] トグルを使用します。相対的な優先順位に従って、最初に試行されるポリシーが決まります。番号が小さいほど優先順位が高くなります。

ステップ 4 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 5 IKEv1 のプロパティを設定します。

- [優先順位]: IKE ポリシーの関連優先順位は 1 ～ 65,535 です。この優先順位によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアは、最も優先順位の高いポリシーで選択されているパラメータをサポートしていない場合、次に小さい優先順位で定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [名前（Name）]：オブジェクトの名前（最大 128 文字）。

- [状態（State）]：IKE ポリシーが有効か無効かを示します。状態を変更するには切り替えをクリックします。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。
- [認証（Authentication）]：2 つのピア間で使用される認証方式。詳細については、使用する認証方式の決定 （6 ページ）を参照してください。
  - [事前共有キー（Preshared Key）]：各デバイスで定義されている事前共有キーを使用します。事前共有キーを使用すると、秘密鍵を2つのピア間で共有し、認証フェーズ中にIKEで使用できます。ピアに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。
  - [証明書（Certificate）]：ピアのデバイス ID 証明書を使用して相互に識別します。認証局に各ピアを登録することによって、これらの証明書を取得する必要があります。また、各ピアでアイデンティティ証明書の署名に使用された、信頼できる CA ルート証明書および中間 CA 証明書もアップロードする必要があります。ピアは、同じ CA または別の CA に登録できます。どちらのピアにも自己署名証明書を使用することはできません。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。オプションの説明については、使用する暗号化アルゴリズムの決定 （3 ページ）を参照してください。
- [Diffie-Hellman グループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密を互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （5 ページ）を参照してください。
- [ハッシュ（Hash）]：メッセージの整合性を確保するために使用されるメッセージ ダイジェストを作成するためのハッシュ アルゴリズム。オプションの説明については、使用するハッシュ アルゴリズムの決定 （4 ページ）を参照してください。
- [有効期間（Lifetime）]：セキュリティ アソシエーション（SA）のライフタイム（120～2147483647 までの秒数、または空白）。このライフタイムを超えると、SAの期限が切れ、2つのピア間で再ネゴシエーションを行う必要があります。一般的に、ライフタイムが（ある程度）短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

ステップ 6 **[OK]** をクリックして変更を保存します。

IKEv2 ポリシーの設定

Internet Key Exchange（IKE; インターネットキーエクスチェンジ）バージョン 2 ポリシー オブジェクトには、VPN 接続を定義する際に IKEv2 ポリシーで必要となるパラメータが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピア

の認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動確立に使用されます。

事前定義済みの IKEv2 ポリシーがいくつか用意されています。ニーズに適したものがあれば、単に [状態（State）] トグルをクリックしてそれらを有効化します。または新しいポリシーを作成して、他のセキュリティ設定の組み合わせを実装することもできます。システム定義されたオブジェクトを編集/削除することはできません。

次の手順では、[オブジェクト（Objects）] ページからオブジェクトを直接作成および編集する方法を説明します。また、オブジェクトの一覧に表示される [新しい IKE ポリシーの作成（Create New IKE Policy）] リンクをクリックすることにより、VPN 接続の IKEv2 設定を編集する際に IKEv2 ポリシー オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [IKE ポリシー（IKE Policies）] を選択します。

ステップ 2 オブジェクト テーブルの上の [IKEv2] を選択し、IKEv2 ポリシーを表示します。

ステップ 3 システム定義されたポリシーの中に要件に合うポリシーがあれば、[状態（State）] トグルをクリックしてそれらを有効化します。

不要なポリシーを無効化する場合にも、[状態（State）] トグルを使用します。相対的な優先順位に従って、最初に試行されるポリシーが決まります。番号が小さいほど優先順位が高くなります。

ステップ 4 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 5 IKEv2 のプロパティを設定します。

- [優先順位]: IKE ポリシーの関連優先順位は 1 ～ 65,535 です。この優先順位によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアは、最も優先順位の高いポリシーで選択されているパラメータをサポートしていない場合、次に小さい優先順位で定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [名前（Name）]：オブジェクトの名前（最大 128 文字）。
- [状態（State）]：IKE ポリシーが有効か無効かを示します。状態を変更するには切り替えをクリックします。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。

- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。許可するすべてのアルゴリズムを選択します。ただし、同じポリシー内に混合モード（AES-GCM）オプションと通常モードオプションの両方を含めることはできません。（通常モードでは整合性ハッシュを選択する必要がありますが、混合モードでは整合性ハッシュを別個に選択することが禁じられています）。システムは、最も強力なアルゴリズムから最も弱いアルゴリズムの順に、一致するものが見つかるまでピアとネゴシエートします。オプションの説明については、使用する暗号化アルゴリズムの決定 （3 ページ）を参照してください。
- [Diffie-Hellman グループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密を互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。許可するアルゴリズムをすべて選択します。システムは、最も強力なグループから最も弱いグループの順に、一致するものが見つかるまでピアとネゴシエートします。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （5 ページ）を参照してください。
- [整合性ハッシュ（Integrity Hash）]：メッセージの整合性を確保するために使用されるメッセージ ダイジェストを作成するためのハッシュ アルゴリズムの整合性部分。許可するアルゴリズムをすべて選択します。システムは、最も強力なアルゴリズムから最も弱いアルゴリズムの順に、一致するものが見つかるまでピアとネゴシエートします。整合性ハッシュを AES-GCM 暗号化オプションと併用することはできません。オプションの説明については、使用するハッシュ アルゴリズムの決定 （4 ページ）を参照してください。
- [疑似ランダム関数（PRF）ハッシュ（Pseudo Random Function (PRF) Hash）]：ハッシュ アルゴリズムの疑似ランダム関数（PRF）部分。このアルゴリズムは IKEv2 トンネル暗号化に必要なキー関連情報とハッシュ操作を取得するために使用されます。IKEv1 では、整合性と PRF アルゴリズムは別々ではありませんが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。許可するアルゴリズムをすべて選択します。システムは、最も強力なアルゴリズムから最も弱いアルゴリズムの順に、一致するものが見つかるまでピアとネゴシエートします。オプションの説明については、使用するハッシュ アルゴリズムの決定 （4 ページ）を参照してください。
- [有効期間（Lifetime）]：セキュリティ アソシエーション（SA）のライフタイム（120～2147483647 までの秒数、または空白）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、ライフタイムが（ある程度）短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

ステップ 6 **[OK]** をクリックして変更を保存します。

IPsec プロポーザルの設定

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2つのピア間のセキュアで論理的な通信パスです。IPsec トンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。IPsec Security Association（SA; セキュリティ アソシエーション）ネゴシエーション中に、ピアでは、両方のピアに共通するトランスフォーム セットが検索されます。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec プロポーザル オブジェクトがあります。

- IKEv1 IPSec プロポーザルを作成する場合、IPSec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成し、選択します。
- IKEv2 IPsec プロポーザルを作成する場合、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。システムは、設定を安全性が最も高いものから最も低いものに並べ替え、その順序に従い一致するものが見つかるまでピアとのネゴシエーションを行います。そのため、IKEv1 のように、許可される各組み合わせを個別に送信するのではなく、許可されるすべての組み合わせを単一のプロポーザルで送信できます。

IKEv1 と IKEv2 IPSec プロポーザルの両方で、カプセル化セキュリティ プロトコル（ESP）が使用されます。これは、認証、暗号化およびアンチリプレイの各サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

（注） IPSec トンネルで暗号化と認証の両方を使用することを推奨します。

次のセクションでは、各 IKE バージョンにおける IPsec プロポーザルの設定方法について説明します。

IKEv1 用 IPsec プロポーザルの設定

IKEv1 IPsec プロポーザル オブジェクトを使用して、IKE フェーズ 2 ネゴシエーション中に使われる IPsec プロポーザルを設定します。IPsec プロポーザルは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。

事前定義済みの IKEv1 IPsec プロポーザルがいくつか用意されています。または新しいプロポーザルを作成して、他のセキュリティ設定の組み合わせを実装することもできます。システム定義されたオブジェクトを編集/削除することはできません。

次の手順では、[オブジェクト（Objects）]ページからオブジェクトを直接作成および編集する方法を説明します。また、オブジェクトの一覧に表示される [新しい IPsec プロポーザルの作成

（Create New IPsec Proposal）] リンクをクリックすることにより、VPN 接続の IKEv1 IPsec 設定を編集する際に IKEv1 IPsec プロポーザル オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、コンテンツ テーブルから [IPsec プロポーザル（IPsec Proposals）] を選択します。

ステップ 2 オブジェクト テーブルの上の [IKEv1] を選択し、IKEv1 IPsec プロポーザルを表示します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 IKEv1 IPsec プロポーザルのプロパティを設定します。

- [名前（Name）]：オブジェクトの名前（最大 128 文字）。
- [モード（Mode）]：IPSec トンネルが動作するモード。
  - [トンネル（Tunnel）] モードでは、IP パケット全体がカプセル化されます。IPSec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これはデフォルトです。トンネル モードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネル モードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPSec が実装される標準の方法です。
  - [トランスポート（Transport）] モードでは、IP パケットの上位層プロトコルだけがカプセル化されます。IPSec ヘッダーは、IP ヘッダーと上位層プロトコル ヘッダー（TCP など）との間に挿入されます。トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポート モードは、レイヤ 2 またはレイヤ 3 のトンネリング プロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。
- [ESP 暗号化（ESP Encryption）]：このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。オプションの説明については、使用する暗号化アルゴリズムの決定 （3 ページ）を参照してください。
- [ESP ハッシュ（ESP Hash）]：認証のために使用するハッシュ アルゴリズムまたは整合性アルゴリズム。オプションの説明については、使用するハッシュ アルゴリズムの決定 （4 ページ）を参照してください。

ステップ 5 **[OK]** をクリックして変更を保存します。

IKEv2 用 IPsec プロポーザルの設定

IKEv2 IPsec プロポーザル オブジェクトを使用して、IKE フェーズ 2 ネゴシエーション中に使われる IPsec プロポーザルを設定します。IPsec プロポーザルは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。

事前定義済みの IKEv2 IPsec プロポーザルがいくつか用意されています。または新しいプロポーザルを作成して、他のセキュリティ設定の組み合わせを実装することもできます。システム定義されたオブジェクトを編集/削除することはできません。

次の手順では、[オブジェクト（Objects）]ページからオブジェクトを直接作成および編集する方法を説明します。また、オブジェクトの一覧に表示される [IPsec プロポーザルの新規作成（Create New IPsec Proposal）] リンクをクリックすることにより、VPN 接続の IKEv2 IPsec 設定を編集する際に IKEv2 IPsec プロポーザル オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、コンテンツ テーブルから [IPsec プロポーザル（IPsec Proposals）] を選択します。

ステップ 2 オブジェクト テーブルの上の [IKEv2] を選択し、IKEv2 IPsec プロポーザルを表示します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 IKEv2 IPsec プロポーザルのプロパティを設定します。

- [名前（Name）]：オブジェクトの名前（最大 128 文字）。
- [暗号化（Encryption）]：このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。許可するアルゴリズムをすべて選択します。システムは、最も強力なアルゴリズムから最も弱いアルゴリズムの順に、一致するものが見つかるまでピアとネゴシエートします。オプションの説明については、使用する暗号化アルゴリズムの決定（3 ページ）を参照してください。
- [整合性ハッシュ（Integrity Hash）]：認証のために使用するハッシュ アルゴリズムまたは整合性アルゴリズム。許可するアルゴリズムをすべて選択します。システムは、最も強力なアルゴリズムから最も弱いアルゴリズムの順に、一致するものが見つかるまでピアとネゴシエートします。オプションの説明については、使用するハッシュ アルゴリズムの決定（4 ページ）を参照してください。

（注）
いずれかの AES-GCM/GMAC オプションを暗号化アルゴリズムとして選択した場合は、NULL 整合性アルゴリズムを選択してください。非 NULL オプションを選択した場合でも、これらの暗号化標準規格は整合性ハッシュを使用しません。

ステップ 5 **[OK]** をクリックして変更を保存します。

サイト間 VPN 接続の確認

サイト間 VPN 接続を設定し、設定をデバイスに展開した後で、システムがリモート デバイスとのセキュリティ アソシエーションを確立することを確認します。

接続を確立できない場合は、デバイス CLI から **ping interface** *interface_name remote_ip_address* コマンドを使用して、VPNインターフェイスを介したリモートデバイスへのパスが存在することを確認します。設定したインターフェイスを介した接続が存在しない場合は、**interface** *interface_name*キーワードをオフにしたまま、接続が別のインターフェイス経由になっていないかどうかを判別します。接続に対して間違ったインターフェイスが選択されている可能性があります。保護されたネットワークに面したインターフェイスではなく、リモートデバイスに面したインターフェイスを選択する必要があります。

ネットワーク パスが存在する場合は、両方のエンドポイントで設定およびサポートされている IKE バージョンとキーを確認し、必要に応じて VPN 接続を調整します。アクセス制御または NAT ルールが接続をブロックしていないことを確認します。

手順

ステップ 1 デバイスCLIにログインします（コマンドラインインターフェイス（CLI）へのログインを参照）。

ステップ 2 **show ipsec sa**コマンドを使用して、IPSecセキュリティアソシエーションが確立されていることを確認します。

ご使用のデバイス（**local addr**）とリモート ピア（**current_peer**）の間に VPN 接続が確立されているはずです。その接続を介してトラフィックを送信すると、パケット（pkts）数が増加します。アクセス リストには、接続のローカル ネットワークおよびリモート ネットワークが表示されます。

たとえば、次の出力は、IKEv2 接続を示しています。

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
```

```
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4

    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4055034/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

次の出力は、IKEv1 接続を示しています。

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
```

```
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
    path mtu 1500, ipsec overhead 74(44), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 077D72C9
    current inbound spi : AC146DEC

  inbound esp sas:
    spi: 0xAC146DEC (2887020012)
       SA State: active
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
       slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
       sa timing: remaining key lifetime (kB/sec): (3914999/28567)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x000007FF
  outbound esp sas:
    spi: 0x077D72C9 (125661897)
       SA State: active
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
       slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
       sa timing: remaining key lifetime (kB/sec): (3914999/28567)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

ステップ 3 **show isakmp sa**コマンドを使用して、IKEセキュリティアソシエーションを確認します。

saキーワードを使用せずに(または代わりに**stats**キーワードを使用して)このコマンドを使用すると、IKE統計情報が表示されます。

たとえば、次の出力は、IKEv2 セキュリティ アソシエーションを示しています。

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify:
PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

次の出力は、IKEv1 セキュリティ アソシエーションを示しています。

```
> show isakmp sa
```

```
IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

サイト間 VPN のモニタリング

サイト間VPN接続をモニタし、トラブルシューティングを行うには、CLIコンソールを開くか、またはデバイスのCLI ログインして、次のコマンドを使用します。

- **show ipsec sa** は VPN セッション（セキュリティ アソシエーション）を表示します。これらの統計は **clear ipsec sa counters** コマンドを使用してリセットできます。
- **show ipsec** *keyword* は IPsec 運用データおよび統計情報を表示します。**show ipsec ?** と入力し、使用可能なキーワードを確認します。
- **show isakmp** は ISAKMP 運用データおよび統計情報を表示します。

サイト間 VPN の例

以下に、サイト間 VPN を設定する例を示します。

NAT からのサイト間 VPN トラフィックの免除

インターフェイスでサイト間 VPN 接続が定義され、そのインターフェイスに NAT ルールが設定されている場合は、オプションで VPN 上のトラフィックを NAT ルールから免除できます。これを行うのは、たとえばVPN接続のリモートエンドで内部アドレスを処理できる場合です。

VPN 接続を作成する際に、[NAT 免除（NAT Exempt）] オプションを選択するとルールを自動的に作成できます。ただし、これが機能するのは、ローカル保護されたネットワークが（ブリッジ グループ メンバーではなく）単一のルーテッド インターフェイス経由で接続される場合だけです。一方、接続内のローカル ネットワークが複数のルーテッド インターフェイスまたは 1 つ以上のブリッジ グループ メンバーの背後に存在する場合は、NAT 免除ルールを手動で設定する必要があります。

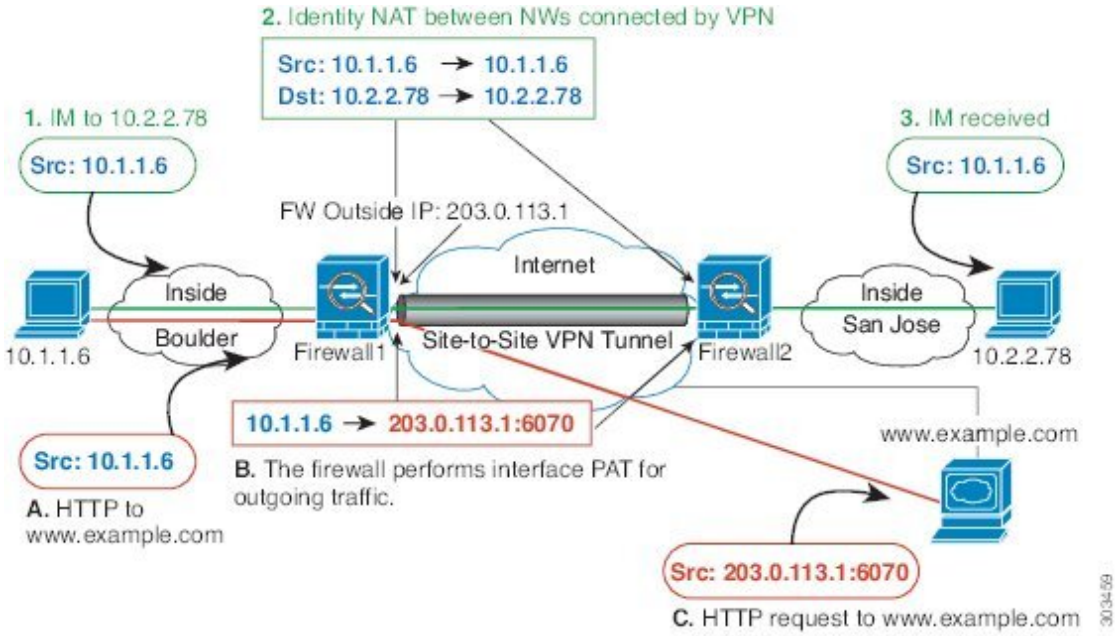
VPN トラフィックを NAT ルールから免除するには、リモート ネットワークを宛先とするローカル トラフィック用のアイデンティティ手動 NAT ルールを作成します。次に、それ以外（インターネットなど）を宛先とするトラフィックに NAT を適用します。ローカル ネットワーク

に複数のインターフェイスが存在する場合は、インターフェイスごとにルールを作成します。さらに、次の推奨事項も考慮してください。

- 接続内に複数のローカル ネットワークが存在する場合、ネットワーク グループ オブジェクトを作成して、それらのネットワークを定義するオブジェクトを保持します。
- VPN に IPv4 ネットワークと IPv6 ネットワークの両方を含める場合は、それぞれに別個のアイデンティティ NAT ルールを作成します。

次の例に、米国ボールダー（Boulder）とサンノゼ（San Jose）のオフィスを接続するサイト間トンネルを示します。インターネットに向かうトラフィック（たとえばボールダーの 10.1.1.6 から www.example.com へ）については、インターネット アクセス用に NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィック（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）については NAT を実行しません。したがって、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は、あるアドレスを同じアドレスに変換するだけです。

図 *1:* サイトツーサイト *VPN* のためのインターフェイス *PAT* およびアイデンティティ *NAT*



次の例は、Firewall1（ボールダー）の設定を示します。この例では、内部インターフェイスがブリッジ グループであることを想定しているため、各メンバー インターフェイスのルールを記述する必要があります。ルーテッド内部インターフェイスが 1 つの場合も複数の場合も、プロセスは同じです。

（注） この例では IPv4 のみと想定しています。VPN に IPv6 ネットワークも含まれる場合は、IPv6 用の並行ルールを作成します。なお、IPv6 インターフェイス PAT を実装することはできないため、PAT に使用する一意の IPv6 アドレスが指定されたホスト オブジェクトを作成する必要があります。

手順

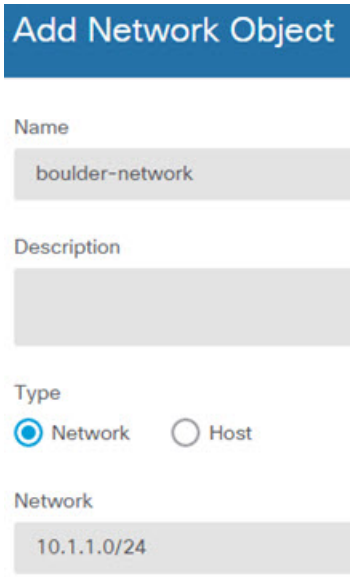
ステップ 1 オブジェクトを作成して、さまざまなネットワークを定義します。

a) [オブジェクト（Objects）] を選択します。

b) コンテンツ テーブルから [ネットワーク（Network）] を選択し、[+] をクリックします。

c) ネットワーク内部の Boulder を識別します。

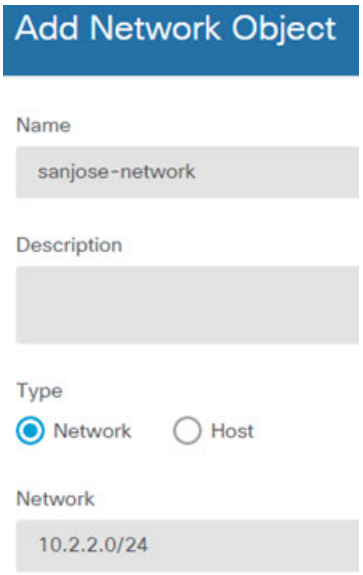
ネットワーク オブジェクトに名前を付け（boulder-network など）、[ネットワーク（Network）] を選択して、ネットワーク アドレス「10.1.1.0/24」を入力します。



d) [OK] をクリックします。

e) [+] をクリックして、内部 San Jose ネットワークを定義します。

ネットワーク オブジェクトに名前を付け（sanjose-network など）、[ネットワーク（Network）] を選択して、ネットワーク アドレス「10.2.2.0/24」を入力します。



f) [OK] をクリックします。

ステップ 2 Firewall1（ボールダー）上で VPN 経由でサンノゼに向かう場合、ボールダー ネットワークの手動アイデンティティ NAT を設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

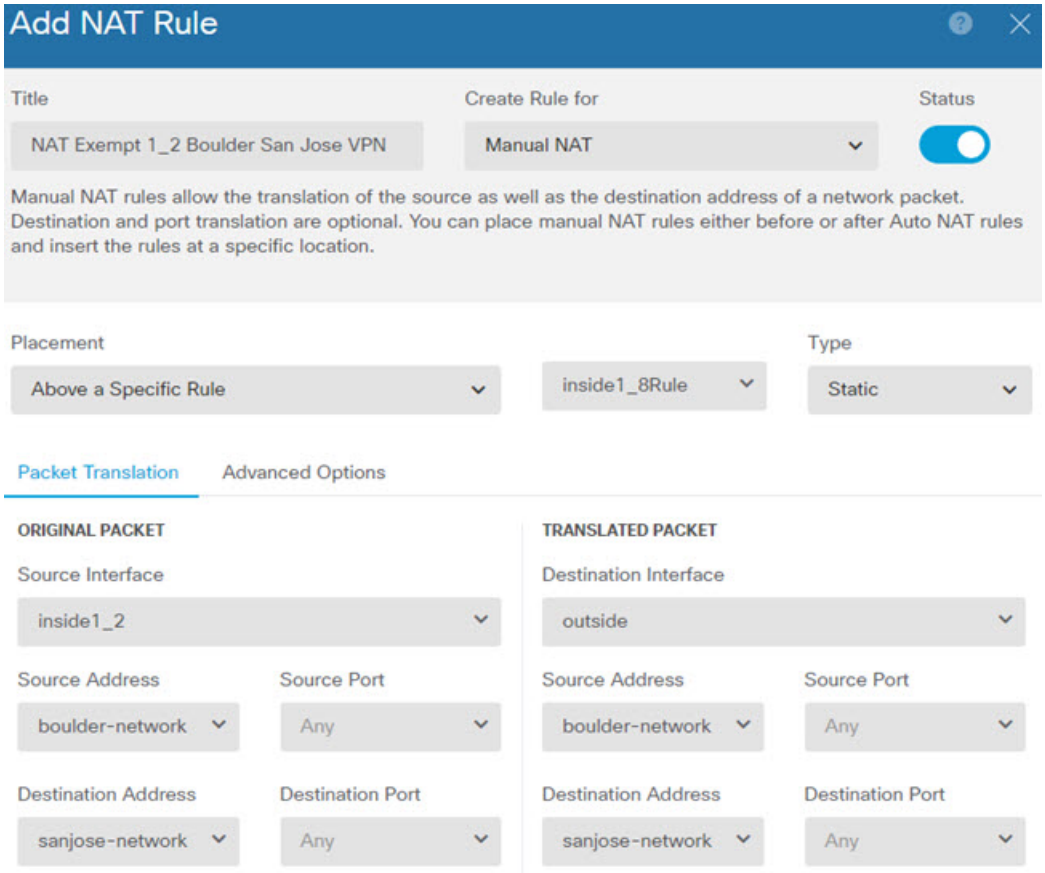
b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = NAT Exempt 1_2 Boulder San Jose VPN（または別の名前）。
- [ルールの作成対象（Create Rule For）] = [手動NAT（Manual NAT）]。
- [配置（Placement）] = [特定のルールの上（Above a Specific Rule）]。[自動NATの前に手動NAT（Manual NAT Before Auto NAT）] セクションの最初のルールを選択します。このルールが、宛先インターフェイスに関するすべての一般的なインターフェイス PAT ルールより前にあることを確認します。そうでない場合、適切なトラフィックにルールが適用されない可能性があります。
- [種類（Type）]：Static。
- [送信元インターフェイス（Source Interface）]：inside1_2。
- [宛先インターフェイス（Destination Interface）]：outside。
- [元の発信元アドレス（Original Source Address）]：boulder-network ネットワーク オブジェクト。
- [変換済み発信元アドレス（Translated Source Address）]：boulder-network ネットワーク オブジェクト。
- [元の宛先アドレス（Original Destination Address）]：sanjose-network ネットワーク オブジェクト。

- [変換済み宛先アドレス（Translated Destination Address）]：sanjose-network ネットワーク オブジェクト。

（注）
宛先アドレスを変換する必要はないため、元の宛先アドレスと変換後の宛先アドレスに同じアドレスを指定することにより、アイデンティティ NAT を設定する必要があります。ポートフィールドはすべて空欄のままにしておきます。このルールは、送信元と宛先の両方にアイデンティティ NAT を設定します。



d) [詳細（Advanced）] タブで、[宛先インターフェイスでプロキシ ARP しない（Do not proxy ARP on Destination Interface）] を選択します。
e) [OK] をクリックします。
f) このプロセスを繰り返して、他の内部インターフェイスにもそれぞれ同等のルールを作成します。

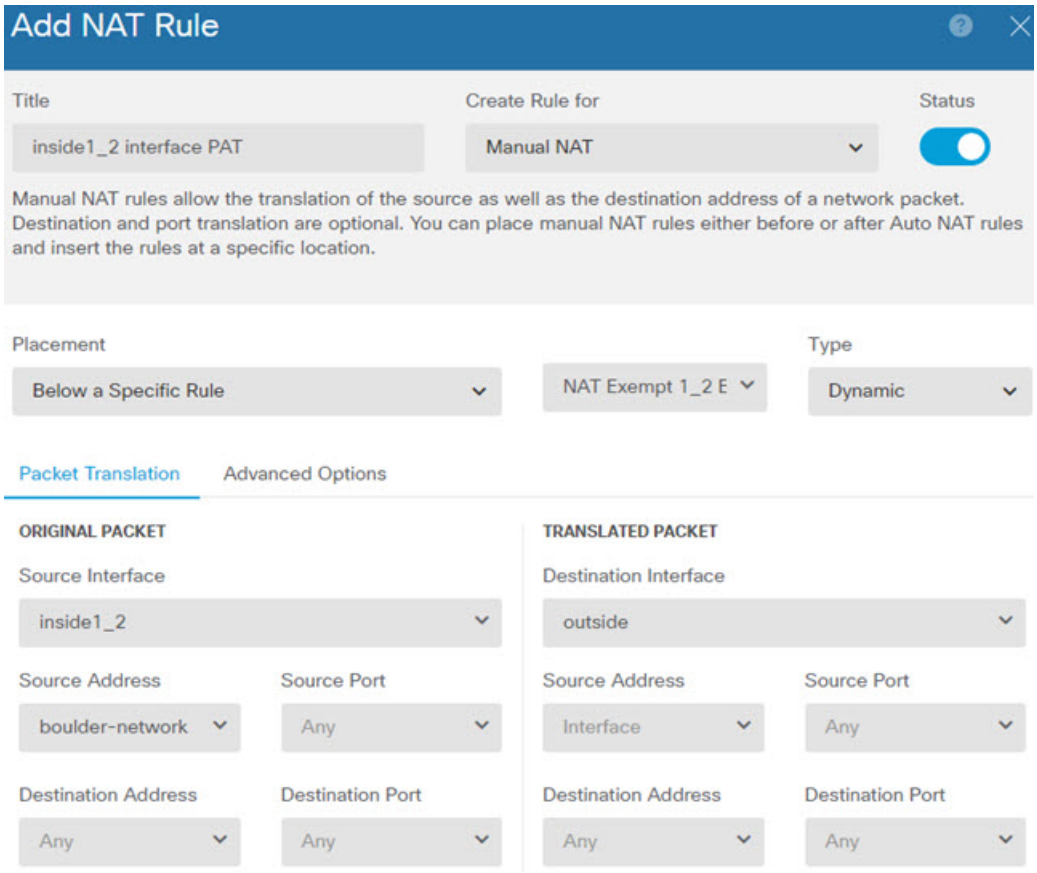
ステップ 3 Firewall1（Boulder）上の内部 Boulder ネットワーク用に、インターネットにアクセスする際の手動ダイナミック インターフェイス PAT を設定します。

（注）
IPv4 トラフィックを対象とする内部インターフェイス用ダイナミック インターフェイス PAT ルールは、初期設定時にデフォルトで作成されるので、既に存在する可能性があります。しかしすべての点を説明するために、ここで設定を示します。これらの手順を完了する前に、内部

インターフェイスとネットワークを対象とするルールが既に存在するかを確認し、存在する場合はこの手順をスキップします。

a) [+] ボタンをクリックします。
b) 次のプロパティを設定します。

- [タイトル（Title）] = inside1_2 インターフェイス PAT（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）] = [手動NAT（Manual NAT）]。
- [配置（Placement）] = [特定のルールの下（Below a Specific Rule）]。[自動NATの前に手動NAT（Manual NAT Before Auto NAT）] セクションで、このインターフェイスのために先に作成したルールを選択します。このルールは任意の宛先アドレスに適用されるので、sanjose-network を宛先として使用するルールはこのルールより前に配置される必要があります。そうしないと sanjose-network ルールが一致しなくなります。デフォルトでは、新しい手動 NAT ルールが [NAT ルールを自動 NAT より優先（NAT Rules Before Auto NAT）] セクションの末尾に配置され、これで十分です。
- [種類（Type）]：Dynamic。
- [送信元インターフェイス（Source Interface）]：inside1_2。
- [宛先インターフェイス（Destination Interface）]：outside。
- [元の発信元アドレス（Original Source Address）]：boulder-network ネットワーク オブジェクト。
- [変換済み発信元アドレス（Translated Source Address）]：Interface。このオプションは、宛先インターフェイスを使用してインターフェイス PAT を設定します。
- [元の宛先アドレス（Original Destination Address）]：any。
- [変換済み宛先アドレス（Translated Destination Address）]：any。



c) [OK] をクリックします。

d) このプロセスを繰り返して、他の内部インターフェイスにもそれぞれ同等のルールを作成します。

ステップ 4 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、または [OK] をクリックして、後でタスク リストや展開履歴を確認します。

ステップ 5 Firewall2（San Jose）も管理している場合は、そのデバイスにも同様のルールを設定できます。

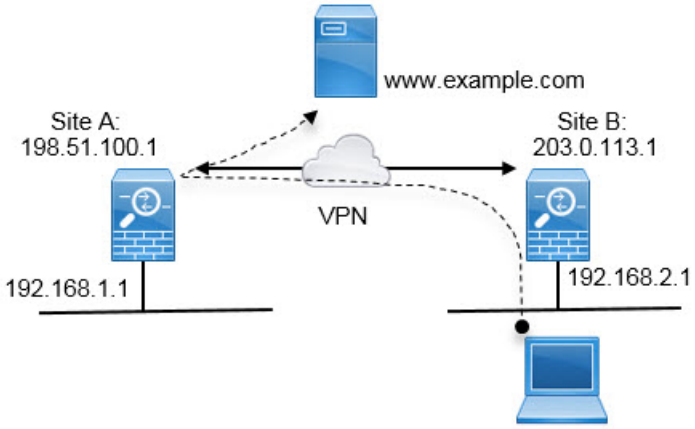
- 手動アイデンティティ NAT ルールの対象は、boulder-network を宛先とする sanjose-network です。Firewall2 内部/外部ネットワーク用に新しいインターフェイス オブジェクトを作成します。

- 手動ダイナミック インターフェイス PAT ルールの対象は、any を宛先とする sanjose-network です。

外部サイト間 VPN ユーザの外部インターフェイスでインターネット アクセスを実現する方法（ヘアピニング）

サイト間VPNでは、リモートネットワーク上のユーザに自分のデバイスを介してインターネットにアクセスさせようとする場合があります。しかし、リモート ユーザは、インターネット（外部インターフェイス）に面している同じインターフェイス上のデバイスにアクセスしているため、インターネット トラフィックを外部インターフェイスからすぐに戻す必要があります。この技術はヘアピニングと呼ばれることがあります。

次の図は、例を示しています。198.51.100.1（メイン サイトのサイト A）と 203.0.113.1（リモート サイトのサイト B）間にサイト間 VPN トンネルが設定されています。リモート サイトの内部ネットワーク（192.168.2.0/24）からのユーザ トラフィックはすべて VPN を通過します。そのため、内部ネットワークのユーザがインターネット上のサーバ（www.example.com など）にアクセスする場合、接続は最初に VPN を通過し、その後 198.51.100.1 インターフェイスからインターネットにルートバックされます。



次の手順では、このサービスの設定方法を説明します。VPN トンネルの両方のエンドポイントを設定する必要があります。

始める前に

この手順では、VPN トラフィックをアクセス コントロール ポリシーの対象とする、VPN トラフィックを許可するためのデフォルト設定を使用していると仮定します。実行中のコンフィギュレーションでは、これは **no sysopt connection permit-vpn** コマンドで表されます。代わりに FlexConfig を介して **sysopt connection permit-vpn** を有効にした場合、または RA VPN 接続プロファイルで [復号されたトラフィックでアクセス制御ポリシーをバイパスする（Bypass Access Control policy for decrypted traffic）] オプションを選択することで、アクセス制御ルールを設定する手順は不要になります。

手順

ステップ 1 （サイト A、メイン サイト）。リモート サイト B へのサイト間 VPN 接続を設定します。

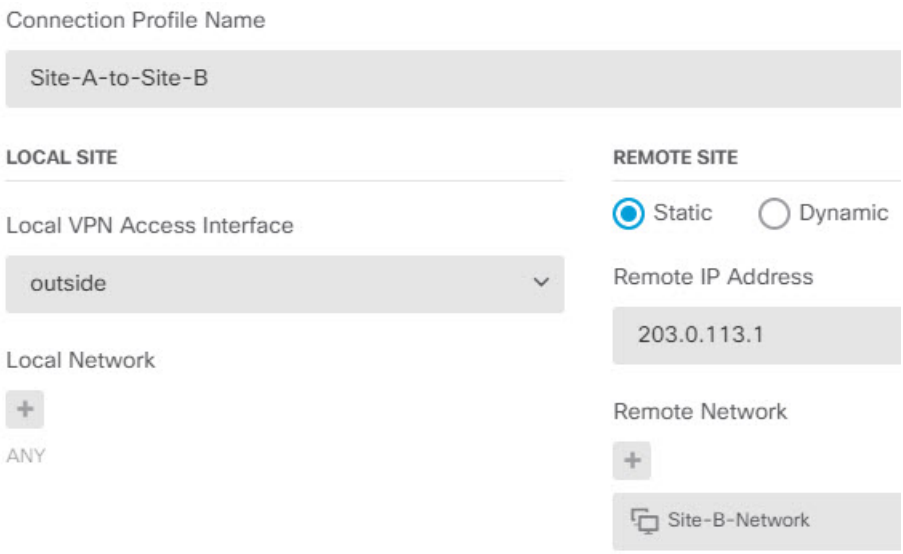
a) **[デバイス（Device）]**をクリックし、次に [サイト間 VPN（Site-to-Site VPN）] グループの [設定の表示（View Configuration）] をクリックします。

b) [+] をクリックして新しい接続を追加します。

c) 次のようにエンドポイントを定義し、[次へ（Next）] をクリックします。

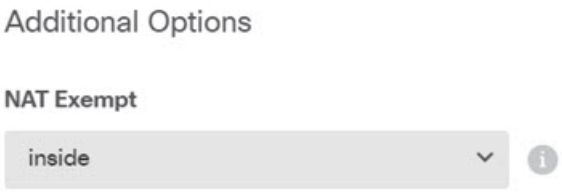
- [接続プロファイル名（Connection Profile Name）]：わかりやすい接続の名前を付けます。例、Connection Profile Name。
- [ローカル VPN アクセス インターフェイス（Local VPN Access Interface）]：外部インターフェイスを選択します。
- [ローカル ネットワーク（Local Network）]：デフォルトの [任意（Any）] のままにします。
- [リモート IP アドレス（Remote IP Address）]：リモート ピアの外部インターフェイスの IP アドレスを入力します。この例では、203.0.113.1 です。
- [リモート ネットワーク（Remote Network）：[+] をクリックして、リモート ピアの保護ネットワークを定義するネットワーク オブジェクトを選択します。この例では、192.168.2.0/24 です。[新しいネットワークの作成（Create New Network）] をクリックして、今すぐオブジェクトを作成できます。

次の図は、最初の手順を示しています。



d) プライバシー設定を定義して、[次へ（Next）] をクリックします。

- [IKE ポリシー（IKE Policy）]：IKE の設定はヘアピニングに影響を及ぼしません。セキュリティのニーズに合わせて IKE バージョン、ポリシー、およびプロポーザルを選択します。入力するローカルとリモートの事前共有キーはメモしてください。リモート ピアの設定時に必要になります。
- [NAT 免除（NAT Exempt）]：内部インターフェイスを選択します。



- [Perfect Forward Secrecy 用 Diffie-Hellman グループ（Diffie-Helman Group for Perfect Forward Secrecy）]：この設定はヘアピニングに影響を及ぼしません。必要に応じて設定します。

e) [完了（Finish）] をクリックします。

接続の概要がクリップボードにコピーされます。接続の概要は、テキストファイルやその他のドキュメントに貼り付けて、リモート ピアの設定に役立てることができます。

ステップ 2 （サイト A、メイン サイト）。外部インターフェイスからのすべての接続の宛先を外部 IP アドレスのポートに変換する NAT ルールを設定します（インターフェイス PAT）。

デバイスの初期設定を完了すると、InsideOutsideNatRule という名前の NAT ルールが作成されます。このルールは、外部インターフェイスを経由してデバイスで終了するすべてのインターフェイスからの IPv4 トラフィックにインターフェイス PAT を適用します。外部インターフェイスは、[任意（Any）] 送信元インターフェイスに含まれているため、ルールはすでに存在している必要があります（ルールを編集または削除している場合を除く）。

次の手順で、必要なルールを作成する方法を説明します。

a) **[ポリシー（Policies）]** > **[NAT]** をクリックします。
b) 次のいずれかを実行します。

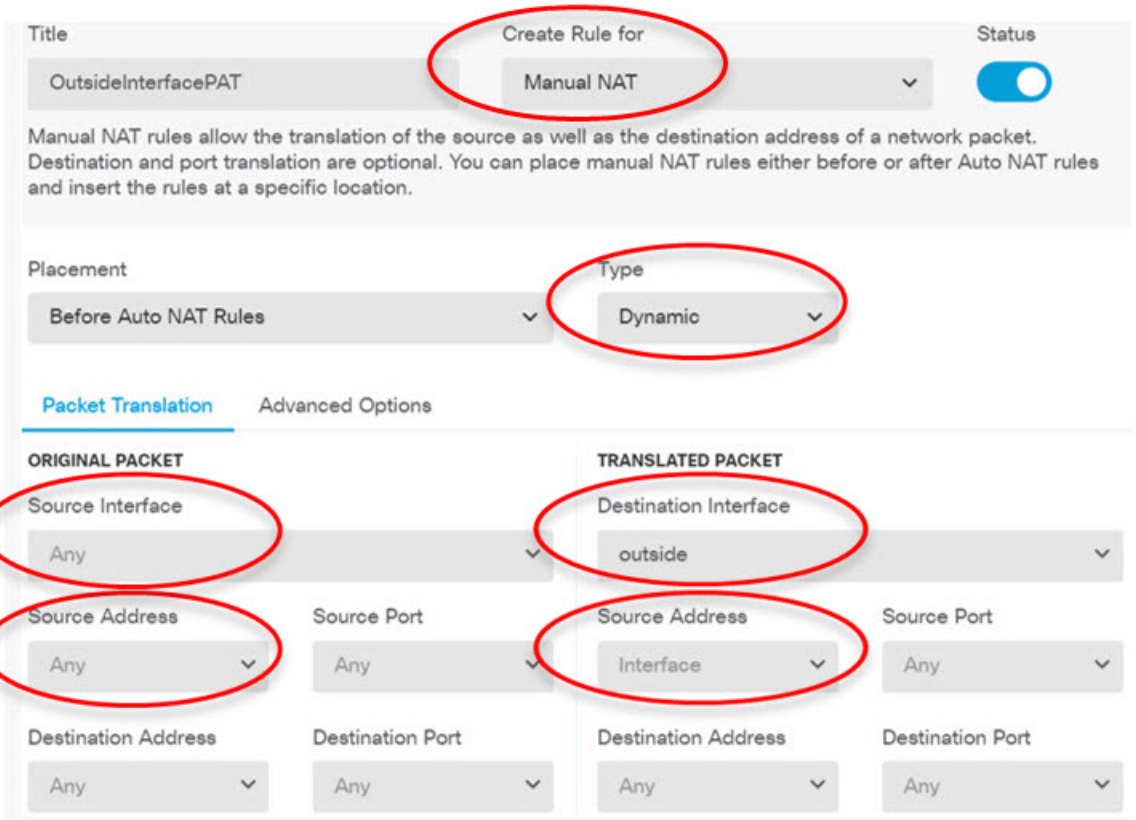
- InsideOutsideNatRule を編集するには、[アクション（Action）] 列にマウス オーバーして、編集アイコン（）をクリックします。
- 新しいルールを作成する場合は、[+] をクリックします。

c) 次のプロパティを指定してルールを設定します。

- [タイトル（Title）]：新しいルールの場合は、スペースを含めずにわかりやすい名前を入力します。例、OutsideInterfacePAT。
- [ルールの作成対象（Create Rule For）]：[手動 NAT（Manual NAT）]。
- [配置（Placement）]：[自動 NAT ルールの前（Before Auto NAT Rules）]（デフォルト）。

- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [元のパケット（Original Packet）]：[送信元アドレス（Source Address）]の場合は、[任意（Any）]またはany-ipv4を選択します。[送信元インターフェイス（Source Interface）]の場合は、デフォルトの[任意（Any）]を必ず選択してください。[元のパケット（Original Packet）]のその他すべてのオプションは、デフォルトの[任意（Any）]のままにします。
- [Translated Packet（変換後のパケット）]：[宛先インターフェイス（Destination Interface）]の場合は、[外部（outside）]を選択します。[変換後のアドレス（Translated Address）]の場合は、[インターフェイス（Interface）]を選択します。[Translated Packet（変換後のパケット）]のその他すべてのオプションは、デフォルトの[任意（Any）]のままにします。

次の図は、発信元アドレスに[任意（Any）]を選択している単純な例を示しています。



d) [OK] をクリックします。

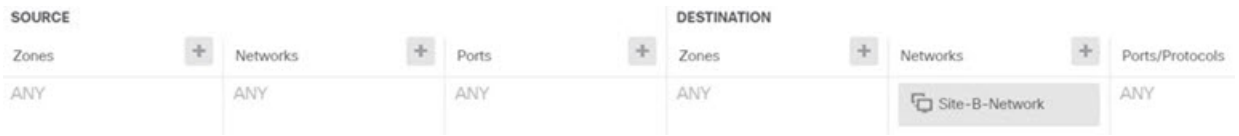
ステップ 3 （サイト A、メイン サイト）。サイト B の保護ネットワークへのアクセスを許可するアクセス制御ルールを設定します。

VPN 接続を作成するだけで、VPN 上のトラフィックが自動的に許可されるわけではありません。使用しているアクセス コントロール ポリシーがリモート ネットワークへのトラフィックを許可している必要があります。

次の手順では、リモート ネットワーク用の固有ルールの追加方法を示します。追加のルールが必要かどうかは、既存のルールによって異なります。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** をクリックします。
b) [+] をクリックして新しいルールを作成します。
c) 次のプロパティを指定してルールを設定します。

- [順序（Order）]：接続と一致し、それらの接続をブロックする可能性があるその他すべてのルールより前の位置をポリシー内で選択します。デフォルトでは、ルールはポリシーの最後に追加されます。後でルールを再配置する必要がある場合は、このオプションを編集するか、テーブルの適切なスロットにルールをドラッグアンドドロップすることができます。
- [タイトル（Title）]：スペースを含めずにわかりやすい名前を入力します。例、Site-B-Network。
- [アクション（Action）]：[許可（Allow）]。このトラフィックのプロトコル違反または侵入を調べない場合は、[信頼（Trust）] を選択できます。
- [送信元または宛先（Source/Destination）] タブ：**[宛先（Destination）]** > **[ネットワーク（Network）]** で、リモート ネットワークの VPN 接続プロファイルに使用しているのと同じオブジェクトを選択します。[送信元と宛先（Source and Destination）] の他のすべてのオプションについては、デフォルトの [任意（Any）] のままにします。



- [アプリケーション（Application）]、[URL]、[ユーザ（Users）] タブ：これらのタブはデフォルトの設定のままにします。つまり、何も選択しません。
- [侵入（Intrusion）]、[ファイル（File）] タブ：必要に応じて、脅威やマルウェアを検査するための侵入ポリシーやファイル ポリシーを選択できます。
- [ロギング（Logging）] タブ：必要に応じて接続ロギングを有効にできます。

d) [OK] をクリックします。

ステップ 4 （サイト A、メイン サイト）。変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、または [OK] をクリックして、後でタスク リストや展開履歴を確認します。ウィンドウを開いたままにすると、展開成功後に保留中の変更がないことが示されます。

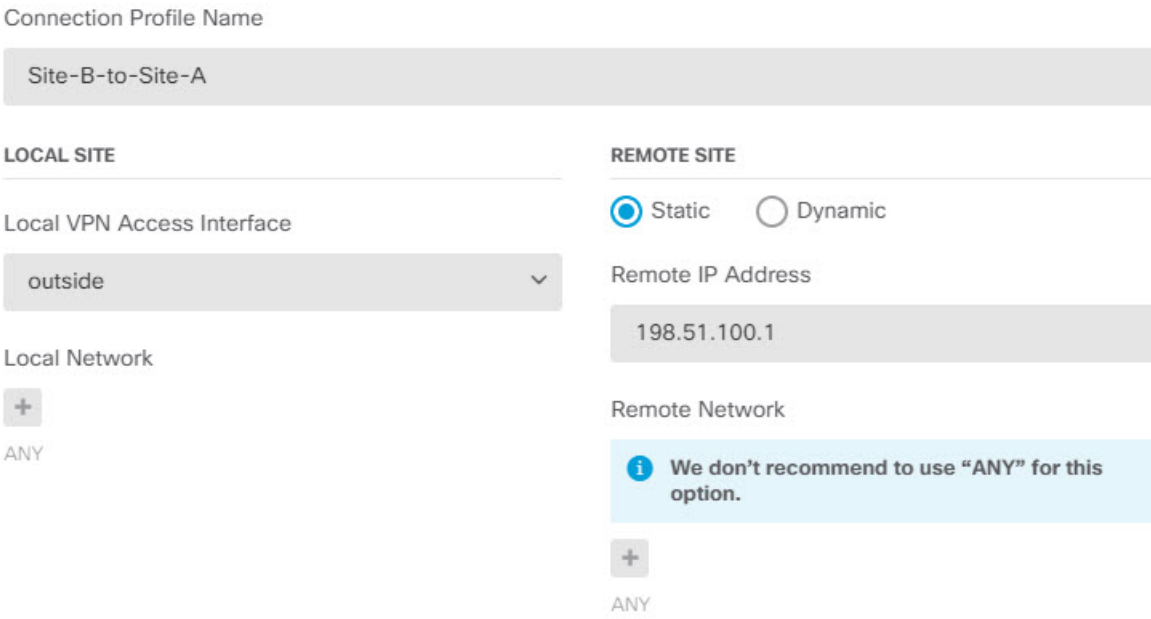
ステップ 5 （サイト B、リモート サイト）リモート サイトのデバイスにログインし、サイト A へのサイト間 VPN 接続を設定します。

サイト A のデバイス設定から取得した接続の概要を使用して、サイト B 側の接続を設定します。

a) **[デバイス（Device）]**をクリックし、次に [サイト間 VPN（Site-to-Site VPN）] グループの [設定の表示（View Configuration）] をクリックします。
b) [+] をクリックして新しい接続を追加します。
c) 次のようにエンドポイントを定義し、[次へ（Next）] をクリックします。

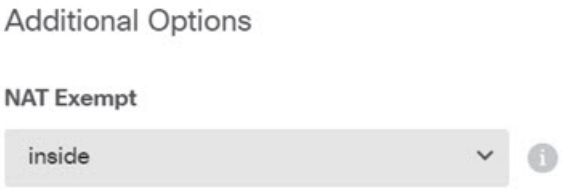
- [接続プロファイル名（Connection Profile Name）]：わかりやすい接続の名前を付けます。例、Site-B-to-Site-A。
- [ローカル VPN アクセス インターフェイス（Local VPN Access Interface）]：外部インターフェイスを選択します。
- [ローカル ネットワーク（Local Network）：[+] をクリックして、ローカルの保護ネットワークを定義するネットワーク オブジェクトを選択します。この例では、192.168.2.0/24 です。[新しいネットワークの作成（Create New Network）] をクリックして、今すぐオブジェクトを作成できます。
- [リモート IP アドレス（Remote IP Address）]：メイン サイトの外部インターフェイスの IP アドレスを入力します。この例では、198.51.100.1 です。
- [リモート ネットワーク（Remote Network）]：デフォルトの [任意（Any）] のままにします。警告は無視します。この使用例には関係ありません。

次の図は、最初の手順を示しています。



d) プライバシー設定を定義して、[次へ（Next）] をクリックします。

- [IKE ポリシー（IKE Policy）]：IKE の設定はヘアピニングに影響を及ぼしません。サイト A の VPN 接続の終端と同じオプションまたは互換性のあるオプションを設定します。事前共有キーは正しく設定する必要があります。サイト A デバイスに設定されている（IKEv2 の）ローカル キーとリモート キーを切り替えます。IKEv1 の場合、キーは 1 つだけで、両方のピアで同一である必要があります。
- [NAT 免除（NAT Exempt）]：内部インターフェイスを選択します。



- [Perfect Forward Secrecy 用 Diffie-Hellman グループ（Diffie-Helman Group for Perfect Forward Secrecy）]：この設定はヘアピニングに影響を及ぼしません。サイト A の VPN 接続の終端で使用されている設定と照合します。

e) [完了（Finish）] をクリックします。

ステップ 6 （サイト B、リモート サイト）保護ネットワークのすべての NAT ルールを削除し、そのサイトからのトラフィックがすべて VPN トンネルを通過するようにします。

サイト A のデバイスではアドレス変換が行われるため、このデバイスで NAT を実行する必要はありません。ただし、個別の状況を確認してください。複数の内部ネットワークがあり、そのすべてがこの VPN 接続に参加しているわけではない場合は、それらのネットワークに必要な NAT ルールを削除しないでください。

a) **[ポリシー（Policies）]** > **[NAT]** をクリックします。
b) 次のいずれかを実行します。

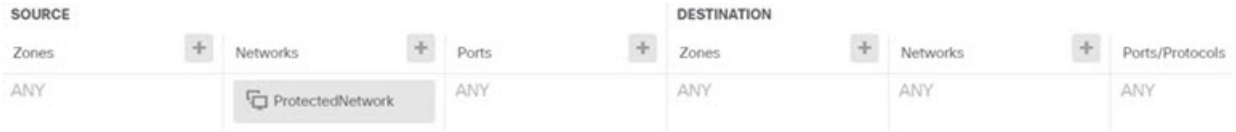
- ルールを削除するには、[アクション（Action）] 列にマウス オーバーして、削除アイコン（）をクリックします。
- ルールを編集して、保護ネットワークに適用されないようにするには、[アクション（Action）] 列にマウス オーバーして、編集アイコン（）をクリックします。

ステップ 7 （サイト B、リモート サイト）保護ネットワークからインターネットへのアクセスを許可するアクセス制御ルールを設定します。

次の例では、保護ネットワークから任意の宛先へのトラフィックが許可されます。これは、ユーザ固有の要件を満たすように調整できます。不必要なトラフィックを除外するブロック ルールをルールの前に配置することもできます。別のオプションとして、サイト A のデバイスにブロック ルールを設定することもできます。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** をクリックします。
b) [+] をクリックして新しいルールを作成します。
c) 次のプロパティを指定してルールを設定します。

- [順序（Order）]：接続と一致し、それらの接続をブロックする可能性があるその他すべてのルールより前の位置をポリシー内で選択します。デフォルトでは、ルールはポリシーの最後に追加されます。後でルールを再配置する必要がある場合は、このオプションを編集するか、テーブルの適切なスロットにルールをドラッグアンドドロップすることができます。
- [タイトル（Title）]：スペースを含めずにわかりやすい名前を入力します。例、Protected-Network-to-any
- [アクション（Action）]：[許可（Allow）]。このトラフィックのプロトコル違反または侵入を調べない場合は、[信頼（Trust）] を選択できます。
- [送信元または宛先（Source/Destination）] タブ：**[送信元（Source）]** > **[ネットワーク（Network）]**で、ローカル ネットワークの VPN 接続プロファイルに使用しているのと同じオブジェクトを選択します。[送信元と宛先（Source and Destination）] の他のすべてのオプションについては、デフォルトの [任意（Any）] のままにします。



- [アプリケーション（Application）]、[URL]、[ユーザ（Users）] タブ：これらのタブはデフォルトの設定のままにします。つまり、何も選択しません。
- [侵入（Intrusion）]、[ファイル（File）] タブ：必要に応じて、脅威やマルウェアを検査するための侵入ポリシーやファイル ポリシーを選択できます。
- [ロギング（Logging）] タブ：必要に応じて接続ロギングを有効にできます。

d) [OK] をクリックします。

ステップ 8 （サイト B、リモート サイト）変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックして、展開が完了するまで待ちます。

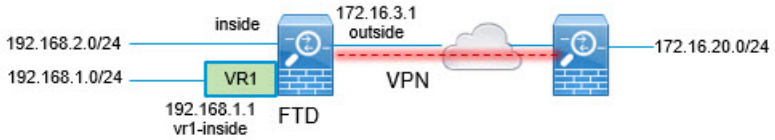
展開が完了するまで待機するか、または [OK] をクリックして、後でタスク リストや展開履歴を確認します。ウィンドウを開いたままにすると、展開成功後に保留中の変更がないことが示されます。

サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

1 つのデバイスに複数の仮想ルータを設定する場合には、グローバル仮想ルータでサイト間 VPN を設定する必要があります。カスタム仮想ルータに割り当てられているインターフェイスにサイト間 VPN を設定することはできません。

仮想ルータのルーティングテーブルはそれぞれ異なるため、サイト間 VPN を介して、カスタム仮想ルータ内でホストされているネットワークとの接続を保護する必要がある場合には、スタティックルートを作成する必要があります。また、前述の付加的なネットワークが含まれるように、サイト間 VPN 接続を更新する必要もあります。

次の例について考えます。この例では、サイト間 VPN は 172.16.3.1 の外部インターフェイスで定義されます。この VPN には、内部インターフェイスがグローバル仮想ルータの一部でもあるため、追加の設定なしで内部ネットワーク 192.168.2.0/24 を含めることができます。ただし、VR1 仮想ルータの一部である 192.168.1.0/24 ネットワークにサイト間 VPN サービスを提供する必要がある場合には、双方向のスタティックルートを設定して、このネットワークをサイト間 VPN 設定に追加する必要があります。



始める前に

この例では、すでに 192.168.2.0/24 ローカルネットワークと 172.16.20.0/24 外部ネットワークの間にサイト間 VPN を設定し、仮想ルータを定義し、インターフェイスを設定して適切な仮想ルータに割り当てていることを前提としています。

手順

ステップ 1 グローバル仮想ルータから VR1 へのルートリークを設定します。

このルートにより、サイト間 VPN の外部（リモート）エンドによって保護されたエンドポイントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできます。

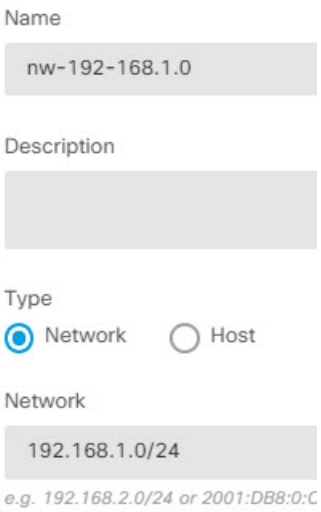
a) **[デバイス（Device）] > [ルーティング（Routing）] > [設定の表示（View Configuration）]** の順に選択します。

b) グローバル仮想ルータの表示アイコン（）をクリックします。

c) グローバルルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

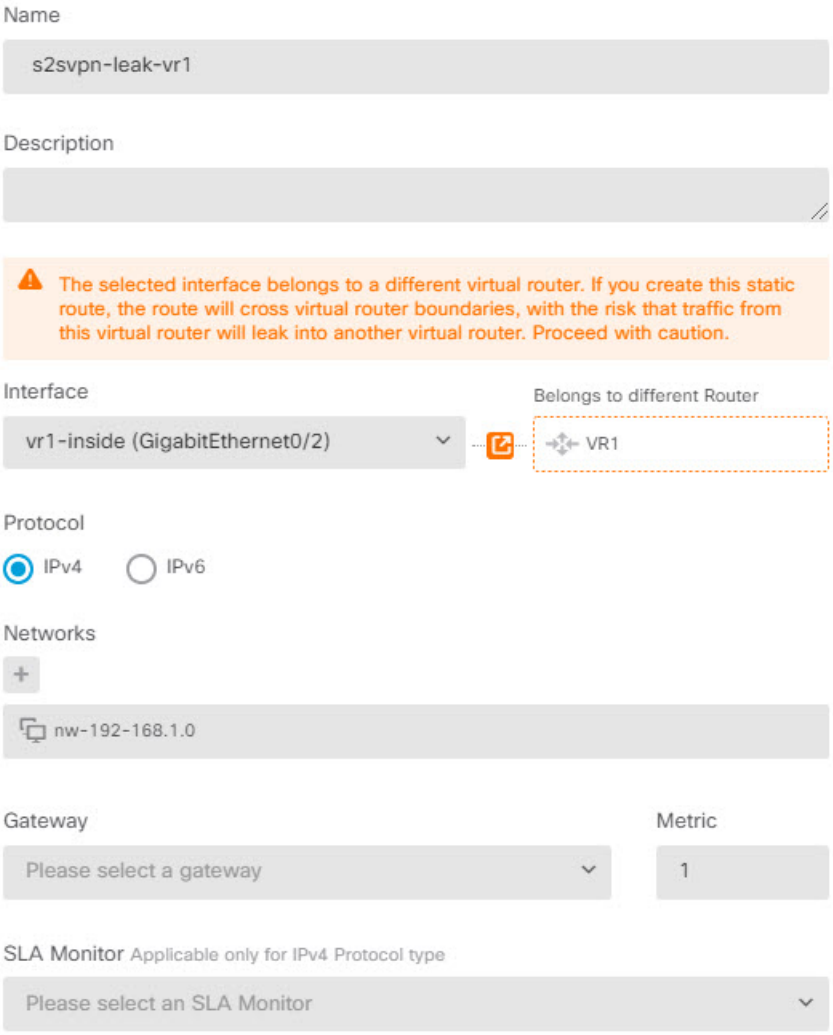
- [名前（Name）]：任意の名前（**s2svpn-leak-vr1** など）を付けることができます。
- [インターフェイス（Interface）]：**vr1-inside** を選択します。

- [プロトコル（Protocol）]：**IPv4** を選択します。
- [ネットワーク（Networks）]：192.168.1.0/24 ネットワークを定義するオブジェクトを選択します。必要な場合には、[新しいネットワークの作成（Create New Network）] をクリックしてオブジェクトを作成します。



- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。



d) [OK] をクリックします。

ステップ 2 VR1 からグローバル仮想ルータへのルートリークを設定します。

このルートにより、192.168.1.0/24 ネットワーク上のエンドポイントは、サイト間 VPN トンネルを通過する接続を開始できます。この例では、リモートエンドポイントが 172.16.20.0/24 ネットワークを保護しています。

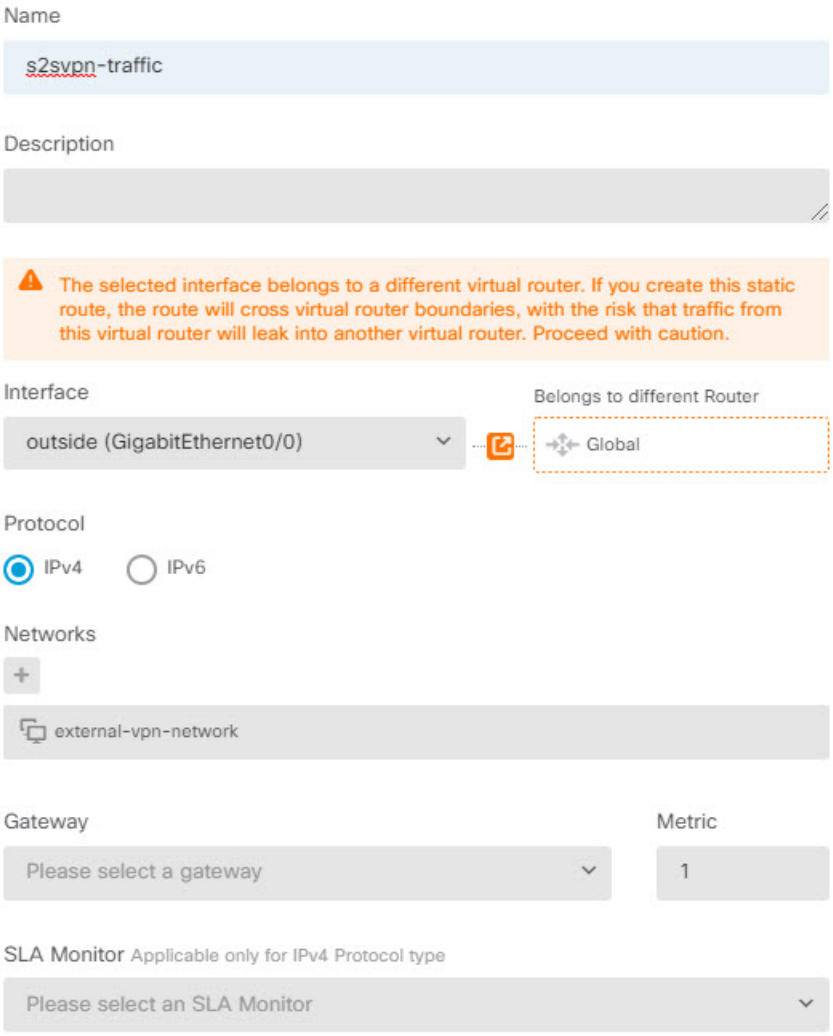
a) 仮想ルータのドロップダウンリストから [VR1] を選択して、VR1 設定に切り替えます。

b) VR1 ルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：任意の名前（**s2svpn-traffic** など）を付けることができます。
- [インターフェイス（Interface）]：**outside** を選択します。
- [プロトコル（Protocol）]：**IPv4** を選択します。

- [ネットワーク（Networks）]：リモートエンドポイントの保護されたネットワークのために作成したオブジェクトを選択します（**external-vpn-network** など）。
- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。



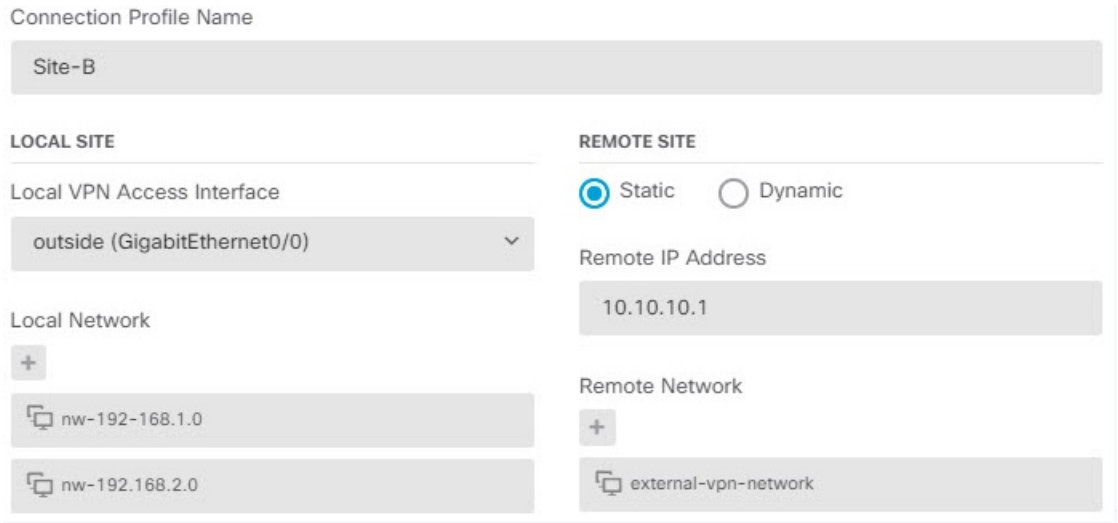
c) [OK] をクリックします。

ステップ 3 192.168.1.0/24 ネットワークをサイト間 VPN 接続プロファイルに追加します。

a) **[デバイス（Device）] > [サイト間VPN（Site-to-Site VPN）] > [設定の表示（View Configuration）]**の順に選択します。

b) 接続プロファイルの編集アイコン（）をクリックします。

c) ウィザードの最初のページで、[ローカルネットワーク（Local Network）] 下の [+] をクリックして、192.168.1.0/24 ネットワークのオブジェクトを追加します。



d) ウィザードを完了します。

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。