



## サイト間 VPN

バーチャルプライベートネットワーク（VPN）は、パブリックソース（インターネットやその他のネットワークなど）を使用して、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ではトンネルを使用して通常のIPパケット内のデータパケットがカプセル化され、IPベースのネットワークを介して転送されます。VPNではプライバシーの確保と認証のために暗号化が使用され、データの整合性が確保されます。

- [VPNの基本（1ページ）](#)
- [サイト間VPNの管理（11ページ）](#)
- [サイト間VPNのモニタリング（31ページ）](#)
- [サイト間VPNの例（31ページ）](#)

## VPNの基本

トンネリングによって、インターネットなどのパブリックTCP/IPネットワークの使用が可能となり、リモートユーザとプライベート企業ネットワークとの間でセキュアな接続を作成できます。各セキュアな接続がトンネルと呼ばれます。

IPsecベースのVPNテクノロジーでは、Internet Security Association and Key Management Protocol（ISAKMPまたはIKE）とIPsecトンネリングを使用して、トンネルを構築し管理します。ISAKMPとIPsecは、次を実現します。

- トンネルパラメータのネゴシエート。
- 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。
- トンネルを経由するデータ転送の管理。
- トンネルエンドポイントまたはルータとしてのインバウンドおよびアウトバウンドのデータ転送の管理。

VPN 内のデバイスは、双方向トンネル 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、それらをカプセル化して、トンネルを作成し、それらをトンネルの他端に送信できます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリックネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベート ネットワーク上の最終宛先に送信することもできます。

サイト間 VPN 接続が確立された後、ローカル ゲートウェイの背後にあるホストは、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と接続できます。接続は、2つのゲートウェイの IP アドレスとホスト名、それらの背後にあるサブネット、および2つのゲートウェイが互いを認証するために使用する方式で構成されます。

## インターネットキー エクスチェンジ (IKE)

インターネットキー エクスチェンジ (IKE) は、IPsec ピアを認証し、IPsec 暗号化キーをネゴシエートして配信し、IPsec セキュリティ アソシエーション (SA) を自動的に確立するため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つのピアが、ピア間のIKE ネゴシエーションの安全性を確保するために使用する一連のアルゴリズムです。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) の場合、IKE ポリシーには単一セットのアルゴリズムとモジュラスグループが含まれます。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 の場合は、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、次を指定します。

- 固有の優先順位 (1 ~ 65,543、1 が最高の優先順位)。
- データを保護し、プライバシーを確保するためのIKE ネゴシエーションの暗号化方式。
- 送信者のIDを保証し、メッセージが伝送中に変更されないように確保するための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る)。
- IKEv2 の場合、IKEv2 トンネル暗号化に必要なキーの材料とハッシュ操作を派生させるためのアルゴリズムとして使用される個別の擬似乱関数 (PRF)。オプションは、ハッシュアルゴリズムで使用されているものと同じです。
- 暗号化キー判別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、暗号化キーとハッシュ キーを派生させます。
- 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すると、ネゴシエーションを開始するピアはリモートピアに有効なポリシーをすべて送信し、リモートピアは優先順位順に自身のポリシーとの一致を検索します。ピアが、暗号化、ハッシュ (IKEv2 の場合は整合性と PRF)、認証、Diffie-Hellman 値を保持し、さらに、送信されたポリシーのライフタイム以下である SA ライフタイムを保持している場合に、IKE ポリシー間に一致が存在します。ライフタイムが同じでない場合は、リモートピア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 を使用するシンプルな IKE ポリシーが唯一有効なポリシーです。より高い優先順位のその他の IKE ポリシーによってより強力な暗号化標準をネゴシエートできますが、DES ポリシーでも正常なネゴシエーションが確保されます。

## VPN 接続の安全性を確保する方法

VPN トンネルは通常、インターネットなどのパブリック ネットワークを経由するため、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 プロポーザルを使用して、暗号化とその他のセキュリティ技術を定義し、適用します。

デバイス ライセンスによって強力な暗号化を適用できる場合は、広範な暗号化とハッシュ アルゴリズム、および Diffie-Hellman グループがあり、その中から選択できます。ただし、一般に、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。効率を損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出します。

シスコでは、どのオプションを選択するかについての特定のガイダンスは提供できません。比較的大規模な企業またはその他の組織内で運用している場合は、すでに、満たす必要がある標準が定義されている可能性があります。定義されていない場合は、時間を割いてオプションを調べてください。

以降のトピックでは、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 プロポーザルに使用する暗号化アルゴリズムを決定する際、選択肢は VPN のデバイスでサポートされるアルゴリズムに限られます。

IKEv2 では、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に並べ替え、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 では、単一のオプションのみ選択できます。

IPsec プロポーザルでは、認証、暗号化、およびアンチリプレイ サービスを提供するカプセル化セキュリティプロトコル (ESP) によってアルゴリズムが使用されます。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の前に ESP というプレフィックスが付けられます。

デバイス ライセンスが強力な暗号化を適用できる場合、次の暗号化アルゴリズムを選択できます。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) Galois/カウンタモードのAdvanced Encryption Standardは、機密性、データの発信元の認証を提供する操作のブロック暗号モードであり、AESよりも優れたセキュリティを提供します。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となるAESモードです。NSA Suite Bは、暗号化強度に関する連邦標準規格を満たすためにデバイスがサポートすべき一連の暗号化アルゴリズムです。
- AES (Advanced Encryption Standard) はDESよりも高度なセキュリティを提供する対称暗号化アルゴリズムであり、計算的には3DESよりも効率的です。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 (データ暗号化標準) : 56ビットキーを使用して暗号化する対称秘密鍵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つのオプションに分かれています。1つは整合性アルゴリズムに使用され、もう1つは擬似乱数関数 (PRF) に使用されます。

IPsec プロポーザルでは、ハッシュアルゴリズムはカプセル化セキュリティプロトコル (ESP) による認証のために使用されます。IKEv2 IPsec プロポーザルでは、これは整合性のハッシュと呼ばれます。IKEv1 IPsec プロポーザルでは、アルゴリズム名にESPというプレフィックスだけでなくHMACというサフィックスも付けられます (ハッシュ方式認証コードを意味する)。

IKEv2では、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に並べ替え、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では、単一のオプションのみ選択できます。

選択可能なハッシュアルゴリズムは、次のとおりです。

- [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。

IKEv2 の設定では、以下の SHA-2 オプションを指定して、より高度なセキュリティを実現できます。NSA Suite B 暗号化仕様を実装するには、次のいずれかを選択します。

- SHA256 : 256 ビットのダイジェストを生成する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を生成する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を生成するセキュアハッシュアルゴリズム SHA 2 を指定します。
- NULL またはなし (NULL、ESP-NONE) : (IPsec プロポーザルのみ) NULL ハッシュアルゴリズム。通常はテスト目的のみに使用されます。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。NULL 以外のオプションを選択した場合、これらの暗号化標準に対しては、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 Security Association (SA : セキュリティアソシエーション) 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 暗号化を選択する場合は、AES で必要な大きいキーサイズをサポートするために、Diffie-Hellman (DH : デフィーヘルマン) グループ 5 以降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 の暗号化の仕様を実装するには、IKEv2 を使用して楕円曲線 Diffie-Hellman (ECDH) オプション : 19、20、21 のいずれか 1 つを選択します。楕円曲線オプションと、2048 ビット係数を使用するグループは、Logjam のような攻撃にさらされる可能性が低くなります。

IKEv2 では、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に並べ替え、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 では、単一のオプションのみ選択できます。

- 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鍵文字列です。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 サーバー) の [拡張] タブにある証明書の [プロパティ (Properties)] 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。

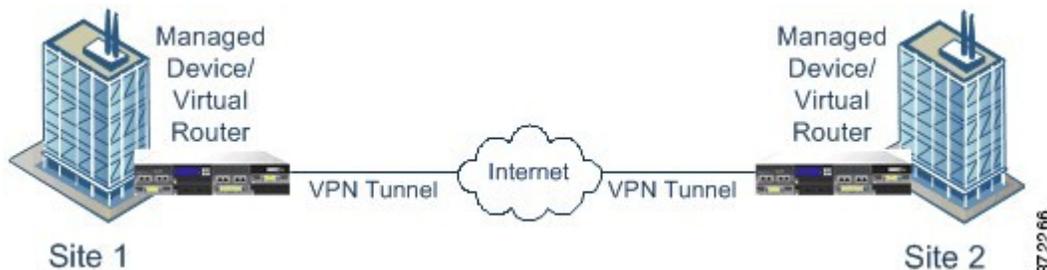
2. ローカルピアのアイデンティティ証明書に署名するために使用された、信頼できる CA 証明書をアップロードします。中間 CA を使用した場合は、ルート証明書と中間証明書を含む完全なチェーンをアップロードします。詳細については、「[信頼できる CA 証明書のアップロード](#)」を参照してください。
3. リモートピアが異なる CA で登録されていた場合、リモートピアのアイデンティティ証明書に署名するために使用した信頼できる CA 証明書もアップロードします。リモートピアを制御する組織から証明書を取得します。中間 CA を使用した場合は、ルート証明書と中間証明書を含む完全なチェーンをアップロードします。

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。

次の図は、一般的なポイントツーポイントの VPN トポロジを示しています。ポイントツーポイントの 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時、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 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ド (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。

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 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

バーチャルプライベート ネットワーク (VPN) は、パブリック ソース (インターネットやその他のネットワークなど) を使用して、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 ではトンネルを使用して通常の IP パケット内のデータ パケットがカプセル化され、IP ベースのネットワークを介して転送されます。VPN ではプライバシーの確保と認証のために暗号化が使用され、データの整合性が確保されます。

ピア デバイスへの VPN 接続を作成できます。接続はすべてポイントツーポイントですが、関連する接続をすべて設定することで、大規模なハブアンドスポークやメッシュ VPN にデバイスを接続できます。

### 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 接続では、暗号化を使用してネットワークのプライバシーが保護されます。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 に登録するときにデバイス上で輸出管理機能を許可するオプションを選択している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、または輸出管理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一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 接続を作成するには、[+] 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。  
まだ接続が存在しない場合でも、[サイト間接続の作成 (Create Site-to-Site Connection)] ボタンはクリックできます。
- 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。その情報をドキュメントに貼り付け、リモート デバイスの管理者に送信して、接続の一端の設定をサポートできます。
- 不要になった接続を削除するには、その接続の[削除 (delete)] アイコン (🗑️) をクリックします。

## サイト間 VPN 接続の設定

リモートデバイスオーナーの協力と許可を得ている場合、ポイントツーポイント VPN 接続を作成し、デバイスを別のデバイスにリンクできます。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各トンネルを定義することで、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

ローカルネットワーク/リモートネットワークの組み合わせごとに、1つの VPN 接続を作成できます。ただし、リモートネットワークが各接続プロファイルで一意である場合は、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 接続を作成するには、[+] ボタンをクリックします。  
まだ接続が存在しない場合でも、[サイト間接続の作成 (Create Site-to-Site Connection)] ボタンはクリックできます。
- 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。

不要になった接続を削除するには、接続の[削除 (delete)] 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)] : この接続の名前で、スペースなしで最大 64 文字までです。例、MainOffice。IP アドレスは名前として使用できません。
- [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 (主にスタティックルート) 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)] : これらのオプションではローカルエンドポイントを定義します。
  - [ローカル VPN のアクセスインターフェイス (Local VPN Access Interface)] : リモートピアが接続できるインターフェイスを選択します。これは通常、外部インターフェイスです。インターフェイスをブリッジグループのメンバーにはできません。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。これらのネットワーク上のユーザーは、この接続を介してリモート ネットワークに到達できます。

(注) これらのネットワークに IPv4 アドレスまたは IPv6 アドレスを使用できますが、接続の各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。1 つの接続の両側で、IPv4 と IPv6 を組み合わせることができます。エンドポイントの保護されたネットワークは重複す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) のどちらかで定義されるか。[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ピアを追加できます。

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。これらのネットワーク上のユーザーは、この接続を介してローカル ネットワークに到達できます。

**ステップ 4** [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) ライセンスにより、どの暗号化プロトコルを選択できるかが決まります。最も基本的なオプション以外のものを選択するには、輸出規制を満たすなど、強力な暗号化が必要です。

- [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) ネゴシエーション時に使用する 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。デバイスがもう1つのピアとの接続のネゴシエーションを試行する場合は、ユーザーが許可したバージョン、およびもう1つのピアが受け入れるバージョンのどちらでも使用されます。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と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1つ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、常に最初に試行されます。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 暗号化キーのネゴシエーションと配布、および 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、有効にしたオブジェクトはすべてのVPNに適用されます。[編集 (Edit) ] をクリックし、IKEバージョンごとに現在グローバルに有効なポリシーを確認し、新しいポリシーを有効化し、作成します。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 トンネルのトラフィックを保護す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を定義します。[編集 (Edit) ] をクリックし、IKEバージョンごとのプロポーザルを選択します。ユーザーに許可するすべてのプロポーザルを選択します。[デフォルトの設定 (Set Default) ] をクリックし、システムデフォルトを選択します。これはエクスポートコンプライアンスに応じて異なります。一致が合意されるまで、最も強いプロポーザルから最も弱いプロポーザルまで、ピアとのネゴシエーションが行われます。詳細については、「[IPsec プロポーザルの設定 \(24 ページ\)](#)」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。これらのキーはIKEv2では異なることがあります。このキーには1～127の英数字を指定できます。
  - (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たキー。このキーには1～127の英数字を指定できます。

- [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 (Create New Object) ]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証明書および中間 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、このウィザードを完了した後に実行できます。
- [IPsec設定 (IPsec Settings) ]: 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 (Lifetime Duration) ]: 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 (Lifetime Size) ]: 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 ~ 2147483647 KB、または空白です。グローバルデフォルトは 4,608,000 キロバイトです。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、ローカルネットワークをホストす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1つのルーテッドインターフェイス (ブリッジグループメンバーではない) 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または1つ以上のブリッジグループのメンバーの背後にある場合、NAT免除ルールを手動で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の詳細については、[NATからのサイト間VPNトラフィックの除外 \(31 ページ\)](#) を参照してください。
- [Perfect Forward Secrecy用Diffie-Helmanグループ (Diffie-Helman Group for Perfect Forward Secrecy) ]: 暗号化されたやり取り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、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、やり取りを以降の復号から保護します。このことは、やり取り全体が記録され、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を有効にする場合、[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と、オプションはIKEv1でサポートされているものに制限されます。オプシ

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** サマリーを確認し、[終了 (Finish) ] をクリックします。

サマリー情報が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 経路による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、スタティック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)] : スライダー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、改行を入れずに 1 行で入力します。
- [トンネルID (Tunnel ID)] : 0 ~ 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 経路による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、外部ユーザが保護されたリモート ネットワーク内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。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。

- リモートネットワーク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 トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザーが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

## 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 エクスチェンジ) 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に対して IKE プロポーザルを定義します。有効にするオブジェクトは、ピアが VPN 接続をネゴシエートするときに使用するものであり、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は、これらの中でどのポリシーを最初に試すかを決定します。数が小さいほど、優先順位が高くなります。ネゴシエーションで両方のピアがサポートできるポリシーを見つけられなければ、接続は確立されません。

IKE グローバル ポリシーを定義するには、各 IKE バージョンを有効にするオブジェクトを選択します。事前定義されたオブジェクトが要件を満たさない場合、セキュリティポリシーを適用する新しいポリシーを作成します。

次に、オブジェクト 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。VPN 接続を編集しているときに IKE ポリシー設定の [編集 (Edit)] をクリックすることで、ポリシーの有効化、無効化および作成が行えます。



(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、次に目次から [IKEポリシー (IKE Policies)] を選択します。

IKEv1 と IKEv2 のポリシーが別のリストに表示されます。

**ステップ 2** 各 IKE バージョンで許可する IKE ポリシーを有効にします。

- a) オブジェクトテーブル上部の [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) 適切なオブジェクトを有効にし、要件を満たしていないオブジェクトを無効にするには、[状態 (State)] トグルをクリックします。

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、要件に合う新しい要件を定義します。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 \(20 ページ\)](#)
- [IKEv2 ポリシーの設定 \(22 ページ\)](#)

- c) 相対的な優先順位が要件を満たすことを確認します。

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。ポリシーが事前定義されたシステムポリシーである場合、優先順位を変更するための独自のバージョンのポリシー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 より優先されます。80 が最も優先順位の高い有効なオブジェクトである場合、これが最初に選択されるポリシーとなります。その後、優先順位が 25 のポリシーを有効にすると、それが最初に選択されるポリシーとなります。

- d) 両方の IKE バージョンを使用する場合、このプロセスを他のバージョンでも繰り返します。

## IKEv1 ポリシーの設定

インターネット キー エクスチェンジ (IKE) 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必要な IKEv1 ポリシーが含まれています。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 セキュリティ アソシエーション (SA) の自動確立に使用されます。

複数の事前定義された IKEv1 ポリシーが存在します。必要に適したポリシーがあれば、[状態 (State)] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

次の手順では、[オブジェクト (Objects)] ページから直接オブジェクトを作成および編集する方法について説明します。IKEv1 設定の編集時に、オブジェクトリストに表示される [新しい IKE ポリシーの作成 (Create New IKE Policy)] リンクをクリックして、IKEv1 ポリシー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** IKEv1 ポリシーを表示するには、オブジェクトテーブル上部の [IKEv1] を選択します。

**ステップ 3** システム定義ポリシーのいずれかが要件を満たす場合には、[状態 (State)] トグルをクリックして有効にします。

不要なポリシーを無効にする場合にも、[状態 (State)] トグルを使用します。番号が小さい方が高い優先順位を持つ相対的な優先順位により、どのポリシーが最初に試行されるかが決定されます。

**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 プロパティを設定します。

- [優先順位 (Priority)] : IKE ポリシーの相対的優先度 (1 ~ 65,535)。このプライオリティによって、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 ピアが、最も高いプライオリティ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、次に低いプライオリティ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。トグルをクリックして状態を変更します。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 ピア間の共有秘密キー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の確保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、一定の限度に達するまで、ライフタイムが短いほど、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

インターネット キー エクスチェンジ (IKE) 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必要な IKEv2 ポリシーが含まれています。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 セキュリティ アソシエーション (SA) の自動確立に使用されます。

複数の事前定義された IKEv2 ポリシーがあります。必要に適したポリシーがあれば、[状態 (State)] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

次の手順では、[オブジェクト (Objects)] ページから直接オブジェクトを作成および編集する方法について説明します。IKEv2 設定の編集時に、オブジェクトリストに表示される [新しい

IKEポリシーの作成 (Create New IKE Policy) ] リンクをクリックして、IKEv2 ポリシー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** IKEv2 ポリシーを表示するには、オブジェクトテーブル上部の [IKEv2] を選択します。

**ステップ 3** システム定義ポリシーのいずれかが要件を満たす場合には、[状態 (State) ] トグルをクリックして有効にします。

不要なポリシーを無効にする場合にも、[状態 (State) ] トグルを使用します。番号が小さい方が高い優先順位を持つ相対的な優先順位により、どのポリシーが最初に試行されるかが決定されます。

**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 プロパティを設定します。

- [優先順位 (Priority) ] : IKE ポリシーの相対的優先度 (1 ~ 65,535) 。このプライオリティによって、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 ピアが、最も高いプライオリティ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、次に低いプライオリティ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。トグルをクリックして状態を変更します。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。有効にするすべてのアルゴリズムを選択します。ただし、同じポリシーに混合モード (AES-GCM) と通常モードのオプションを含めることはできません (通常モードには整合性ハッシュの選択が必要ですが、混合モードは個別の整合性ハッシュの選択を無効化します)。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認でき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 ピア間の共有秘密キー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。許可するすべてのアルゴリズムを選択します。システムは、最も強いグループから始めて最も弱いグループに至るまで、適合するものが確認でき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の確保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。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。整合性ハッシュは、AES-GCM 暗号化オプションでは使用されません。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。
- [擬似ランダム関数 (PRF) ハッシュ (Pseudo Random Function (PRF) Hash) ] : IKEv2 トンネル暗号化に必要なキー材料とハッシュ操作を得るためのアルゴリズムとして使用されるハッシュアルゴリズムの擬似ランダム関数 (PRF) 部分。IKEv1 では、整合性と PRF アルゴリズムは別ですが、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。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認でき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、一定の限度に達するまで、ライフタイムが短いほど、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) の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て選択します。
- IKEv2 IPsec プロポーザルを作成する際に、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、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

カプセル化セキュリティプロトコル (ESP) は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。これは認証、暗号化、および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。



(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。

次に、各 IKE バージョンの IPsec プロポーザルの設定方法を説明します。

## IKEv1 の 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 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、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。

定義済みの複数の IKEv1 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトは、編集または削除できません。

次の手順では、[オブジェクト (Objects)] ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv1 IPsec 設定を編集している間に、オブジェクトリストに表示される [新規 IPsec プロポーザルの作成 (Create New IPsec Proposal)] リンクをクリックして、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、目次から [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にある [IKEv1] を選択して、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 : 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。これがデフォルトです。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 : 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)] : 認証に使用するハッシュ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 の 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 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、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。

定義済みの複数の IKEv2 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトは、編集または削除できません。

次の手順では、[オブジェクト (Objects)] ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv2 IPsec 設定を編集している間に、オブジェクトリストに表示される [新規 IPsec プロポーザルの作成 (Create New IPsec Proposal)] リンクをクリックして、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、目次から [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 テーブルの上にある [IKEv2] を選択して、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。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認でき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)] : 認証に使用するハッシュまたは整合性アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認でき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) 暗号化アルゴリズムとしていずれかの AES-GCM/GMAC オプションを選択する場合は、ヌル整合性アルゴリズムを選択する必要があります。これらの暗号化基準では、ヌル以外のオプションを選択している場合でも、整合性ハッシュは使用されません。

**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 (CLI (コマンドラインインターフェイス) 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が、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, #rcv 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 にログインして、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 トラフィックの除外

インターフェイスでサイト間 VPN 接続が定義されていて、かつそのインターフェイス向けの NAT ルールを指定している場合、NAT ルールから VPN 上のトラフィックを任意で除外できます。この操作は、VPN 接続のリモートエンドが内部アドレスを処理できる場合に行うと便利です。

VPN 接続を作成するときに、[NATを除外 (NAT Exempt)] オプションを選択すると、ルールが自動的に作成されます。ただし、これはローカルで保護されたネットワークが単一のルーテッドインターフェイス（ブリッジグループメンバーではない）を介して接続されている場合のみ動作します。その代わりに、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、NAT 免除ルールを手動で設定する必要があります。

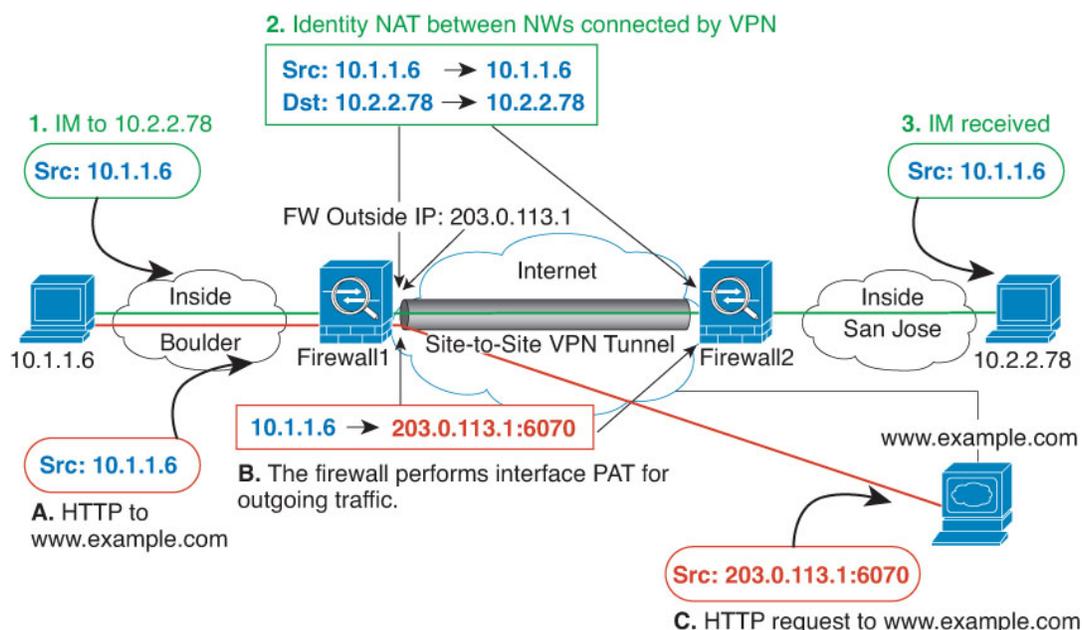
NAT ルールから VPN トラフィックを除外するには、宛先がリモートネットワークのときにローカルトラフィックの手動アイデンティティ NAT ルールを作成します。次に、任意の宛先（インターネットなど）のトラフィックに NAT を適用します。ローカルネットワークに複数のインターフェイスがある場合、各インターフェイスにルールを作成します。次の点も考慮してください。

- 接続内に複数のローカルネットワークがある場合、ネットワークを定義するオブジェクトを保持するネットワーク オブジェクト グループを作成します。

- 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、それぞれに個別のアイデンティティ NAT ルールを作成します。

次の例では、ボールドーとサンノゼのオフィスを接続するサイトツーサイトトンネルを示します。インターネットに渡すトラフィックについて（たとえばボールドーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために 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については（たとえば、ボールドーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、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 は同じアドレスにアドレスを変換します。

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（ボールドー）の設定を示します。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と仮定するため、各メンバーインターフェイスにルールを記述する必要があります。ルーティングされた内部インターフェイスが1つある場合も複数ある場合も、プロセスは同じです。



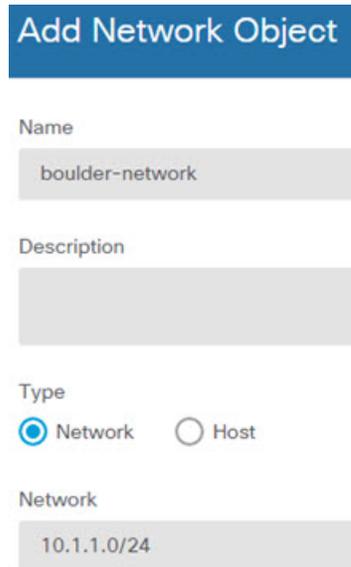
(注) この例では、IPv4 のみと仮定します。VPN に IPv6 ネットワークも含まれる場合、IPv6 にはパラレルルールを作成します。IPv6 インターフェイス PAT は実装できないため、PAT を使用するには固有の IPv6 アドレスを持つホストオブジェクトを作成する必要があることに注意してください。

## 手順

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

- a) [オブジェクト (Objects) ] を選択します。
- b) 目次から [ネットワーク (Network) ] を選択し、[+] をクリックします。
- c) ネットワーク内でボールダーを特定します。

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。



**Add Network Object**

Name  
boulder-network

Description

Type  
 Network  Host

Network  
10.1.1.0/24

- d) [OK] をクリックします。
- e) [+] をクリックしてサンノゼの内部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。

**Add Network Object**

Name  
sanjose-network

Description

Type  
 Network     Host

Network  
10.2.2.0/24

f) [OK] をクリックします。

**ステップ 2** Firewall1 (ボールドー) 上で VPN 経由でサンノゼに向かう場合、ボールドー 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の一般的なインターフェイス PAT ルールの前に来ていることを確認してください。そうでないと、ルールが正しいトラフィックに適用されない場合があります。
  - [タイプ (Type)] = [スタティック (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)] = [外部 (outside)]
  - [元の発信元アドレス (Original Source Address)] = boulder-network のネットワーク オブジェクト (boulder-network network object)。
  - [変換済みの発信元アドレス (Translated Source Address)] = boulder-network のネットワーク オブジェクト (boulder-network network object)。
  - [元の宛先アドレス (Original Destination Address)] = sanjose-network のネットワーク オブジェクト (sanjose-network network object)。

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

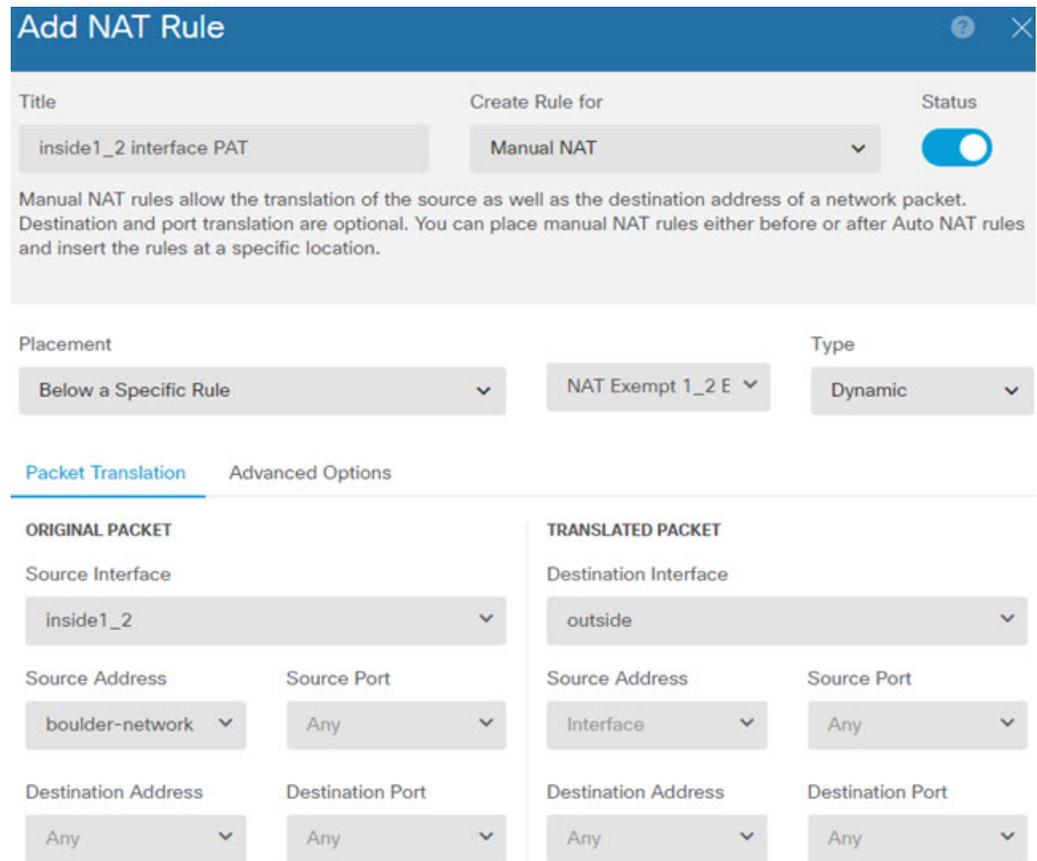
(注) 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート (Port)] フィールドはすべて空白のままにします。このルールは、送信元と宛先の両方のアイデンティティ NAT を設定します。

- [詳細 (Advanced)] タブで [宛先インターフェイスでプロキシARPなし (Do not proxy ARP on Destination interface)] を選択します。
- [OK] をクリックします。
- 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

**ステップ 3** Firewall1 (ボールダー) 上でボールダーの内部ネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。

(注) これらは初期設定時にデフォルトで作成されるため、内部インターフェイスにはすでに IPv4 トラフィックをカバーするダイナミック インターフェイス PAT ルールがある可能性があります。ただし、この設定は説明を完結させるために示しています。こ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カバーするルールがすでに存在していることを確認して、存在している場合はこの手順をスキップしてください。

- 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ため、sanjose-network を宛先として使用するルールはこのルールの前に来る必要があります。そうでなければ、sanjose-network ルールは永遠に一致することがありません。デフォルトでは、新しい手動 NAT ルールは [自動NATの前にNAT ルール (NAT Rules Before Auto NAT) ] セクションの最後に配置されますが、これでも問題ありません。
  - [タイプ (Type) ] = [ダイナミック (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) ] = [外部 (outside) ]
  - [元の発信元アドレス (Original Source Address) ] = boulder-network のネットワーク オブジェクト (boulder-network network object)。
  - [変換済み発信元アドレス (Translated Source Address) ] = [インターフェイス (Interface) ]。このオプションは、宛先インターフェイスを使用するインターフェイス PAT を設定します。
  - [元の宛先アドレス (Original Destination Address) ] = 任意 (any)。
  - [変換済みの宛先アドレス (Original Destination Address) ] = 任意 (any)。



- c) [OK] をクリックします。
- d) 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

**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、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

**ステップ 5** Firewall2 (サンノゼ) の管理を行っている場合、そのデバイスに同様のルールを設定できません。

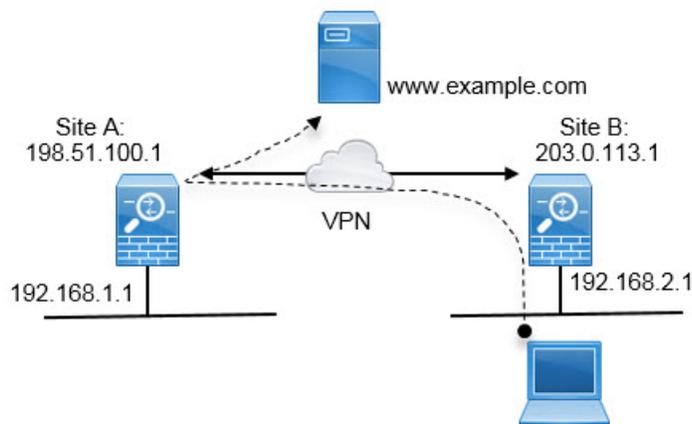
- 手動アイデンティティ NAT ルールは、宛先が boulder-network の場合は sanjose-network 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイスオブジェクトを作成します。

- 手動ダイナミック インターフェイス PAT ルールは、宛先が「任意」の場合は sanjose-network 向けになります。

## 外部インターフェイスで外部のサイト間 VPN ユーザーにインターネット アクセスを提供する方法（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たい場合があります。ただし、インターネットに接続している同一インターフェイス（外部インターフェイス）上のデバイスにリモート ユーザーがアクセスしているため、インターネットトラフィックが外部インターフェイスの外側からそのまま返される必要があります。この手法はヘア ピニングと呼ばれる場合もあります。

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について説明します。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、[サイト間VPN (Site-to-Site VPN)] グループで [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。[ネットワークの新規作成 (Create New Network)] をクリックしてすぐにオブジェクトを作成できます。

次に、最初の手順の状況を図で示します。

Connection Profile Name

Site-A-to-Site-B

<p><b>LOCAL SITE</b></p> <hr/> <p>Local VPN Access Interface</p> <p>outside</p> <p>Local Network</p> <p>+</p> <p>ANY</p>	<p><b>REMOTE SITE</b></p> <hr/> <p><input checked="" type="radio"/> Static <input type="radio"/> Dynamic</p> <p>Remote IP Address</p> <p>203.0.113.1</p> <p>Remote Network</p> <p>+</p> <p>Site-B-Network</p>
--	---

- d) プライバシー ポリシーを定義し、[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 ピニングに影響を与えません。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 (inside)] インターフェイスを選択します。

### Additional Options

#### NAT Exempt

inside

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

- e) [終了 (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送信されたすべての接続を外部 IP アドレス (インターフェイス PAT) のポートに変換するよう NAT ルールを設定します。

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経由でデバイスを抜ける任意のインターフェイスから、インターフェイス PAT を IPv4 トラフィックに充当します。外部インターフェイスは「任意の」送信元インターフェイスに含まれるため、必要なルールは、編集または削除していない限り、すでに存在しています。

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、[編集 (edit)] アイコン (🔍) をクリックします。
- ルールを新規作成するには、[+] ボタンをクリックします。

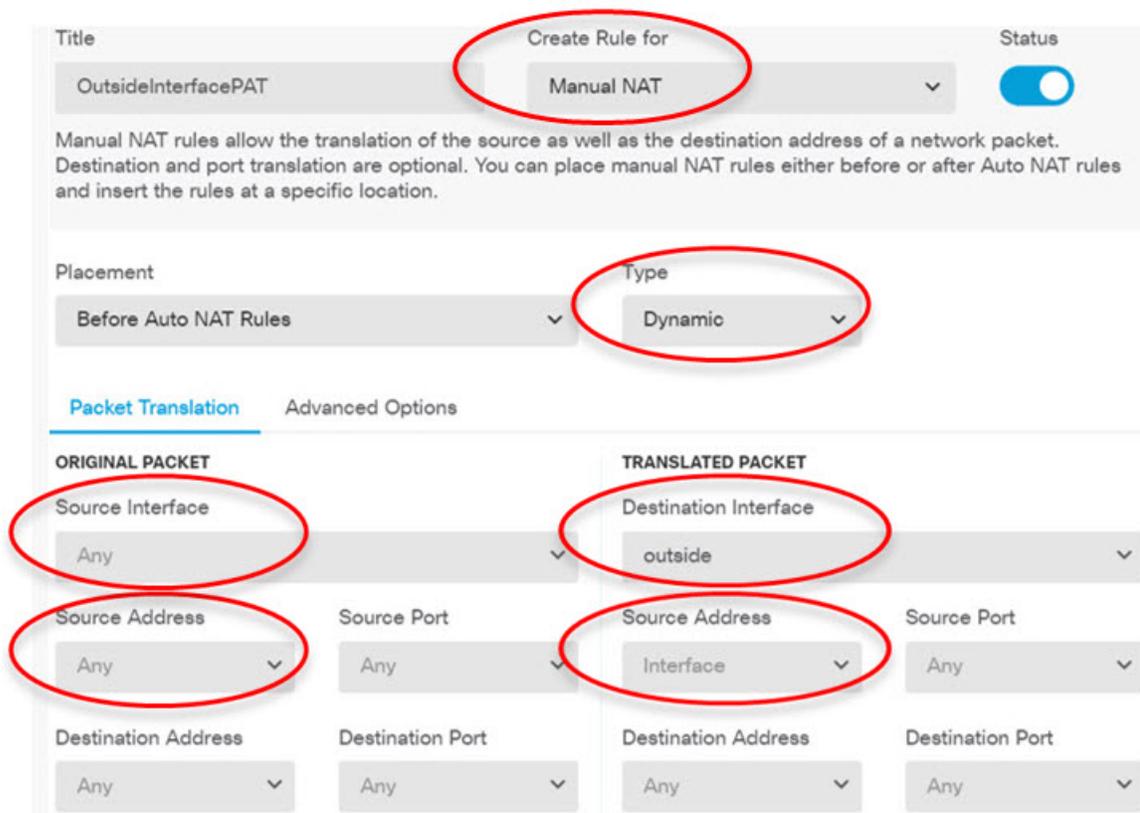
- c) 次のプロパティを使用してルールを設定します。

- [タイトル (Title)] : 新しいルールのわかりやすい名前をスペースを含めず入力します。たとえば、**OutsideInterfacePAT** と入力します。
- [ルールの作成先 (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 packets (Original Packet)] : [送信元アドレス (Source Address)] で [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)] で、[任

意 (Any) ] (デフォルト) を選択していることを確認します。[元の packets (Original Packet) ]の他の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。

- [変換後の packets (Translated Packet) ] : [宛先インターフェイス (Destination Interface) ]で、[外部 (outside) ]を選択します。[変換後のアドレス (Translated Address) ]で、[インターフェイス (Interface) ]を選択します。[変換後の packets (Translated Packet) ]の他の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) ]を選択したシンプル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) 次のプロパティを使用してルールを設定します。
  - [順序 (Order) ] : ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。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。ルールの位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。
  - [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。

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	ANY	ANY	ANY	Site-B-Network	ANY

- [アプリケーション (Application) ]、[URL]、および [ユーザー (Users) ] タブ : これらのタブではデフォルトの設定（何も選択しない）のままにします。
  - [侵入 (Intrusion) ]、[ファイル (File) ] タブ : オプションで、脅威またはマルウェアを検索する侵入またはファイル ポリシーを選択できます。
  - [ロギング (Logging) ] タブ : オプションで接続の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、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。ウィンドウをアクティブのままにすると、展開が正常に終了した後、保留中の変更はないことが表示されます。

**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、[サイト間VPN (Site-to-Site VPN)] グループで [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。[ネットワークの新規作成 (Create New Network)] をクリックしてすぐに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。

次に、最初の手順の状況を図で示します。

Connection Profile Name

Site-B-to-Site-A

LOCAL SITE

Local VPN Access Interface

outside

Local Network

+

ANY

REMOTE SITE

Static  Dynamic

Remote IP Address

198.51.100.1

Remote Network

**i** We don't recommend to use "ANY" for this option.

+

ANY

- d) プライバシー ポリシーを定義し、[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 ピニングに影響を与えません。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（inside）] インターフェイスを選択します。

### Additional Options

#### NAT Exempt

inside

- [Perfect Forward SecrecyのDiffie Helman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) [終了（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（delete）] 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（edit）] 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。これは独自の要件に合わせて調整できます。不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置くことができます。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。

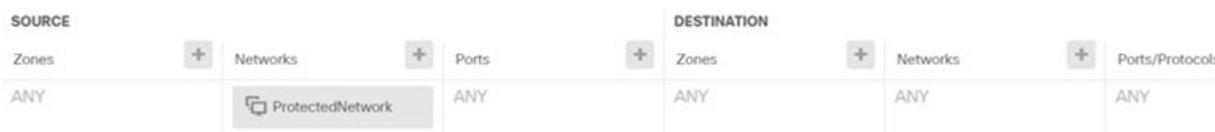
b) [+] をクリックして新しいルールを作成します。

c) 次のプロパティを使用してルールを設定します。

- [順序（Order）] : ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。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。ルールを位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。

- [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]、および[ユーザー (Users) ] タブ: これらのタブではデフォルトの設定 (何も選択しない) のままにします。
- [侵入 (Intrusion) ]、[ファイル (File) ] タブ: オプションで、脅威またはマルウェアを検索する侵入またはファイル ポリシーを選択できます。
- [ロギング (Logging) ] タブ: オプションで接続の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。

- 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。



- [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。

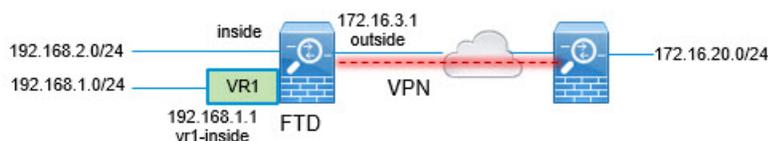
展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。ウィンドウをアクティブのままにすると、展開が正常に終了した後、保留中の変更はないことが表示されます。

## 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。

次の例を考えてみます。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。

Name  
nw-192-168.1.0

Description

Type  
 Network  Host

Network  
192.168.1.0/24  
e.g. 192.168.2.0/24 or 2001:DB8:0:C

- [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。

Name

s2svpn-leak-vr1

Description

**⚠ The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.**

Interface

vr1-inside (GigabitEthernet0/2) Belongs to different Router

VR1

Protocol

IPv4  IPv6

Networks

+

nw-192-168.1.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

d) [OK] をクリック

**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。

- 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。
- 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。

Name

s2svpn-traffic

Description

**⚠ The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.**

Interface

outside (GigabitEthernet0/0) Belongs to different Router

Global

Protocol

IPv4  IPv6

Networks

+ external-vpn-network

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

- c) [OK] をクリック

**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。

- [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。
- 接続プロファイルの編集アイコン (🔗) をクリックします。
- 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) ] の下の [+] 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。

Connection Profile Name

Site-B

---

**LOCAL SITE**

Local VPN Access Interface

outside (GigabitEthernet0/0) ▼

Local Network

+

nw-192-168.1.0

nw-192.168.2.0

**REMOTE SITE**

Static  Dynamic

Remote IP Address

10.10.10.1

Remote Network

+

external-vpn-network

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。