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

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 プロポーサルを使用して、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。

- 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-GMAC—（IKEv2 IPsec プロポーザルのみ）。Advanced Encryption Standard のガロア メッセージ認証コード（GMAC）は、データ発信元認証だけを行う操作のブロック暗号モードです。これは AES-GCM の一種であり、データを暗号化せずにデータ認証が行えます。AES-GMAC 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。
- 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。
- 3DES（トリプル DES）：56 ビット キーを使用して暗号化を 3 回行います。異なるキーを使用してデータの各ブロックを 3 回処理するため、DES よりも安全です。ただし、使用するシステム リソースが多くなり、DES よりも速度が遅くなります。
- 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。3DES よりも高速であり、使用するシステム リソースも少ないですが、安全性も劣ります。堅牢なデータ機密保持が必要ない場合、およびシステム リソースや速度が重要である場合には、DES を選択します。
- Null：ヌル暗号化アルゴリズムは暗号化なしで認証します。通常はテスト目的にのみ使用されます。

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)：160 ビットのダイジェストを生成します。SHA は、総当たり攻撃に対して、MD5 よりも高い耐性があります。ただし、SHA は MD5 よりもリソース消費量が大きくなります。最大レベルのセキュリティを必要とする実装には、SHA ハッシュ アルゴリズムを使用してください。

  Standard 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。

- MD5 (Message Digest 5)：128 ビットのダイジェストを生成します。MD5 は処理時間が短いため、全体的なパフォーマンスが SHA より高速ですが、SHA より強度は低いと考えられています。
- 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/GMAC 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、以下にリストされているすべてのグループをサポートしていません。

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。

- 2：Diffie-Hellman グループ 2（1024 ビット Modular Exponential（MODP）グループ）。このオプションは優れた保護とは見なされなくなりました。

- 5：Diffie-Hellman グループ 5（1536 ビット MODP グループ）。以前は 128 ビット キーに対する優れた保護と見なされていましたが、このオプションは優れた保護と見なされなくなりました。
- 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。
- 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）。
- 24：Diffie-Hellman グループ 24（2048 ビット MODP グループおよび 256 素数位数サブグループ）。このオプションは推奨されなくなりました。

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 接続でピアを認証することもできます。

事前共有キー

事前共有キーは、接続内のそれぞれのピアに設定されている秘密鍵の文字列です。これらのキーは、認証フェーズ中に IKE によって使用されます。IKEv1 の場合は、それぞれの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と比べて拡張性に劣ります。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 を使用することは便利ですが、必須ではありません。

   VPN 接続を確立するために自己署名証明書を使用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、[拡張（Extensions）] タブ（Windows CA サーバ）の証明書の [プロパティ（Properties）] ダイアログボックスで確認できま

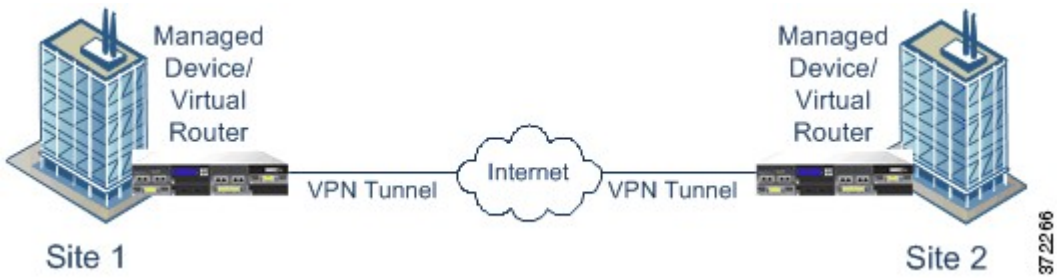
す。この拡張機能のデフォルトは、IP セキュリティ IKE 中間ですが、これは FDM を使用して設定されたサイト間 VPN では機能しません。

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 が使用されていた場合は、ルートおよび中間証明書を含むチェーン全体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 が使用されていた場合は、ルートおよび中間証明書を含むチェーン全体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

Firepower 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 アドレスがわからない場合でも、ピアにサイト間 VPN 接続を作成できます。これは、次の状況で役立ちます。

- 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 アドレスを含むリモート 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したピア B にセキュアな接続を確立する必要がある場合、接続 A の終端に静的 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 で接続を作成する際に、ピアのアドレスが動的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。

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。

（注） 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。

手順

ステップ 1 [デバイス（Device）] をクリックします。 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 （9 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 （9 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。

（注） 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。

手順

ステップ 1 [デバイス（Device）] をクリックします。 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、[サイト間接続の作成（Create Site-to-Site Connection）] ボタンをクリックします。

- 既存の接続を編集するには、接続の [編集（edit）] 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。たとえば、「MainOffice」など。名前として IP アドレスは使用できません。
- [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。
  - [ローカルネットワーク（Local Network）]：[+] 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のいずれに定義されているか（たとえば、DHCP を使用して）。[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。
  - [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。
  - [リモートネットワーク（Remote Network）]：[+] をクリックして、VPN 接続に参加する必要があるリモート ネットワークを特定するネットワーク 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 [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） 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。必要に応じて、いずれかまたは両方のオプションを選択します。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 （13 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トが行われます。詳細については、IPsec プロポーザルの設定 （18 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。これらの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 では異なる場合があります。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。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。認証局（CA）から取得した証明書である必要があります。自己署名証明書を使用すること

はできません。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 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。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。

- [NAT免除（NAT Exempt）]：VPN トラフィックをローカル VPN アクセス インターフェイス上の NAT ポリシーから除外するかどうか。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 （25 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 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 経由によるトラフィックの許可 （12 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。

構成を配置した後、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がセキュリティ アソシエーションを確立することを確認します。サイト間 VPN 接続の確認 （22 ページ）を参照してください。

サイト間 VPN 経由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。これは、トラフィックに対する接続イベントは発生せず、したがって統計ダッシュボードでは VPN 接続が反映されないことも意味します。

  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。

- 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。

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 （14 ページ）
- IKEv2 ポリシーの設定 （16 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。

次に、[オブジェクト（Objects）]ページで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。これらのキーを使用すると、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。各ピアを認証局で登録することで、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。ピアは同じまたは別の CA に登録することができます。いずれ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。

次に、[オブジェクト（Objects）] ページで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の編集や削除はできません。

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の編集や削除はできません。

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を介し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。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 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。これらの統計情報は **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参照します。
- **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。

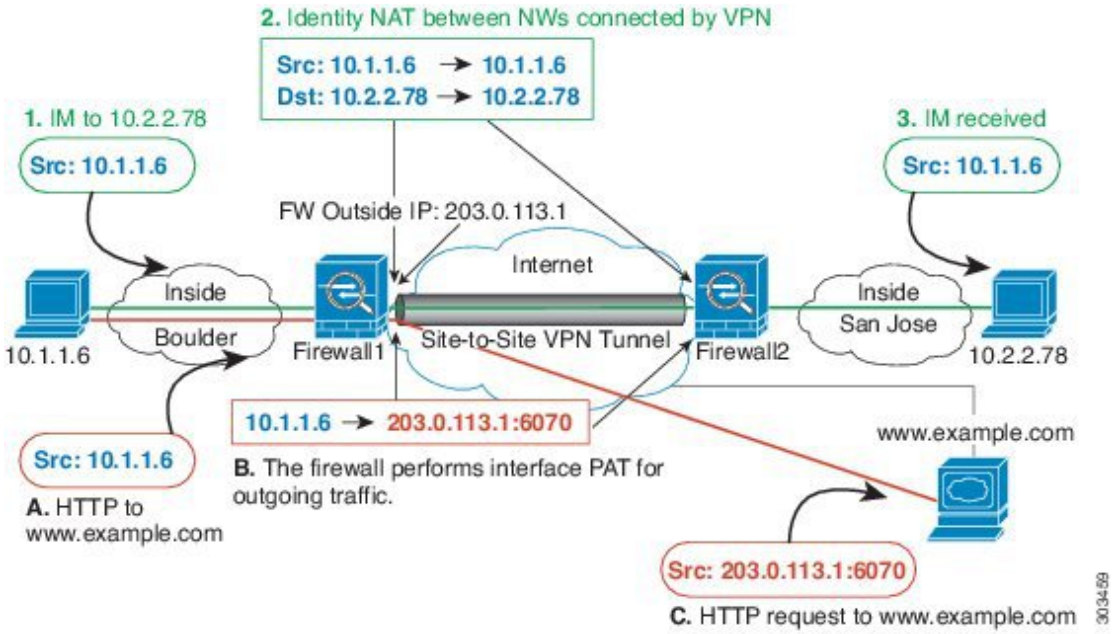
NAT ルールから VPN トラフィックを除外するには、宛先がリモート ネットワークのときにローカル トラフィックの手動アイデンティティ NAT ルールを作成します。次に、任意の宛先

（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、ボールダ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（たとえばボールダーの 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、ボールダーの 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（ボールダー）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

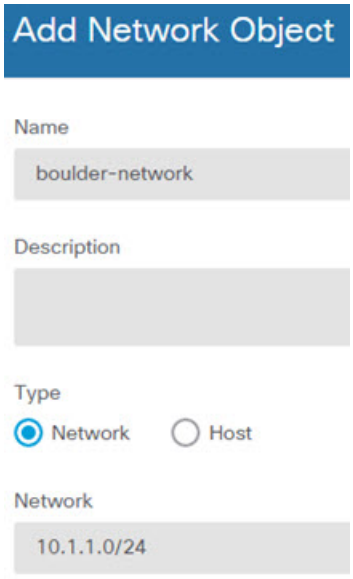
ステップ 1 さまざまなネットワークを定義するには、オブジェクトを作成します。

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。

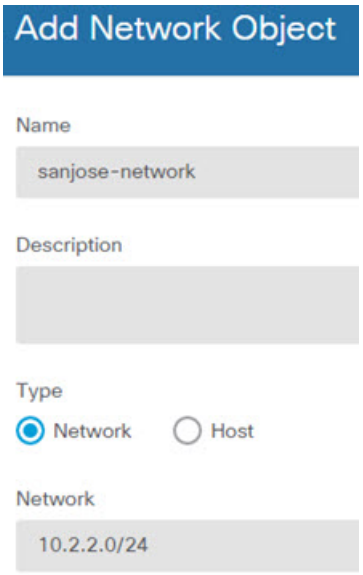
ネットワーク オブジェクトに名前を付け（boulder-network など）、[ネットワーク（Network）] を選択して、ネットワーク アドレス 10.1.1.0/24 を入力します。



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。



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。

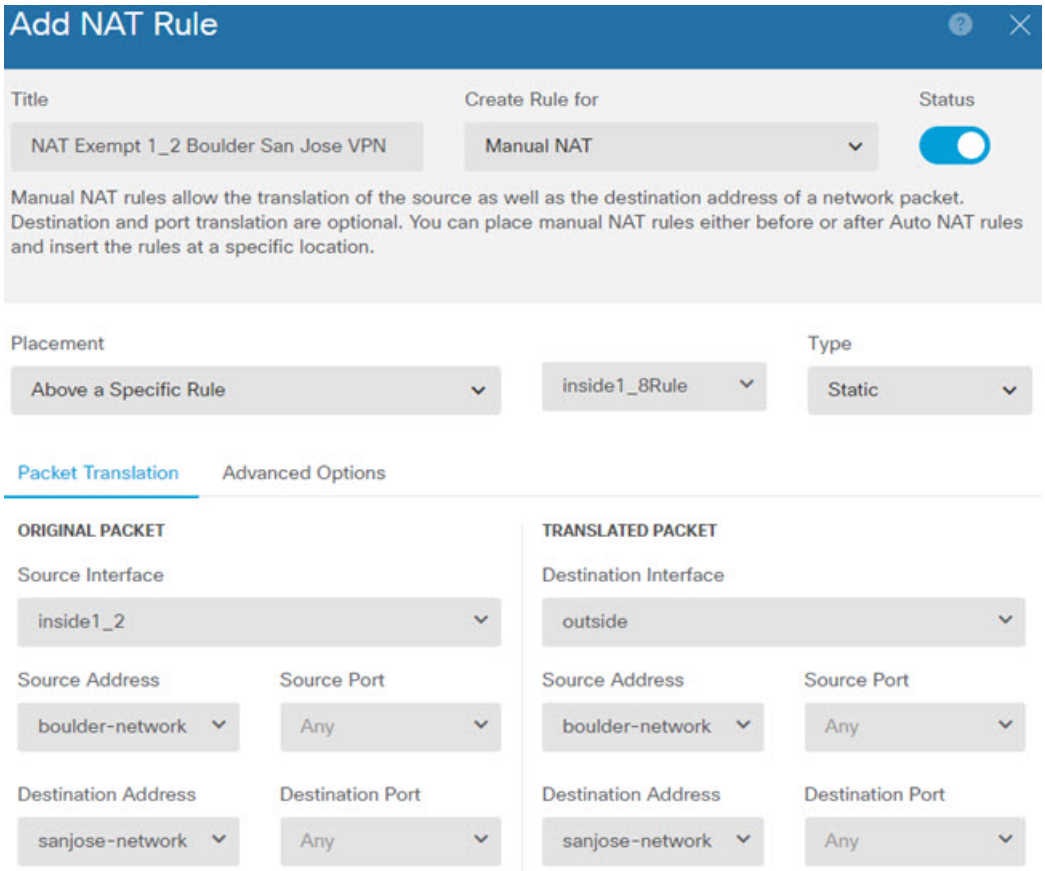
b) [+] ボタンをクリックします。

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。



d) [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。

e) [OK] をクリックします。

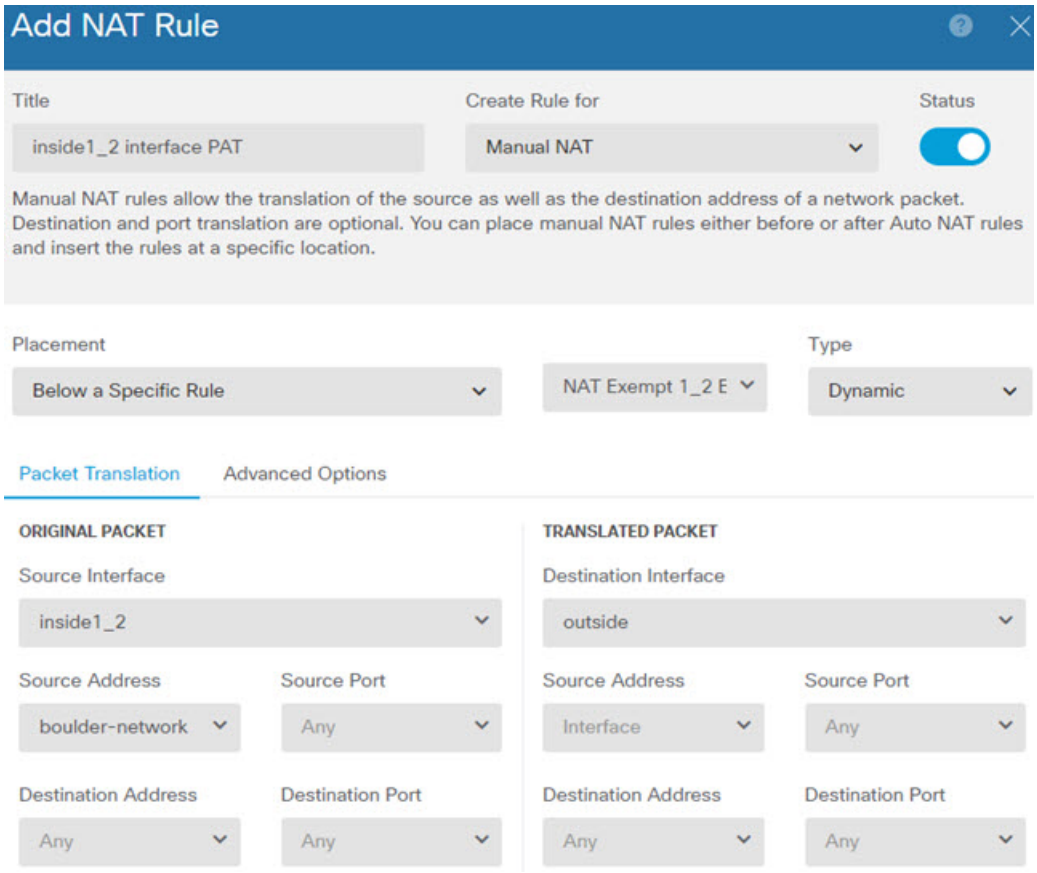
f) 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

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す。

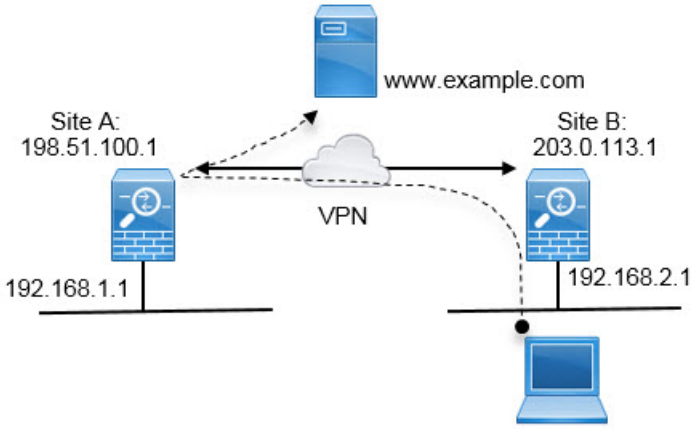
- 手動アイデンティティ NAT ルールは、宛先が boulder-network の場合は sanjose-network 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイス オブジェクトを作成します。

- 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。

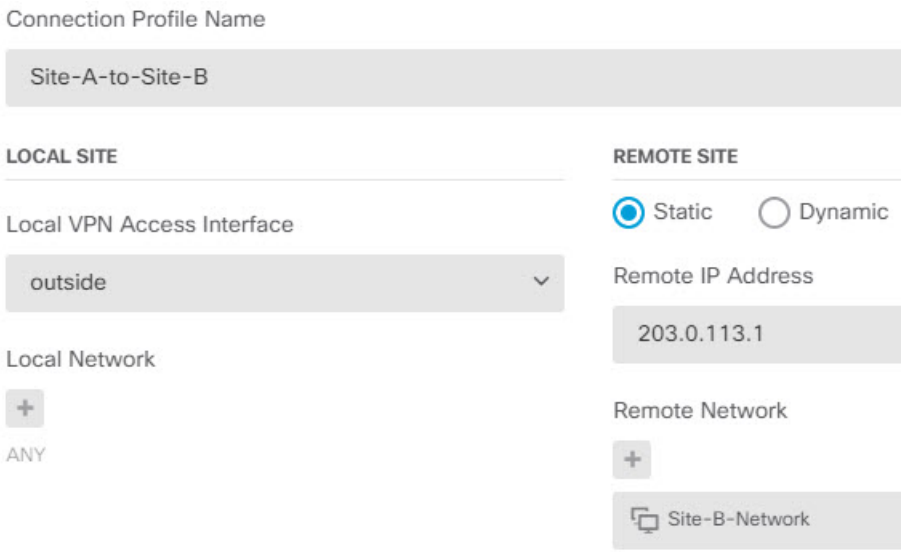
a) [デバイス（Device）] をクリックし、[サイト間VPN（Site-to-Site VPN）] グループで [設定の表示（View Configuration）] をクリックします。

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。

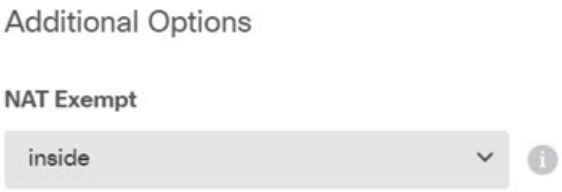


d) プライバシー ポリシーを定義し、[次へ（Next）] をクリックします。

- [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。



- [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。

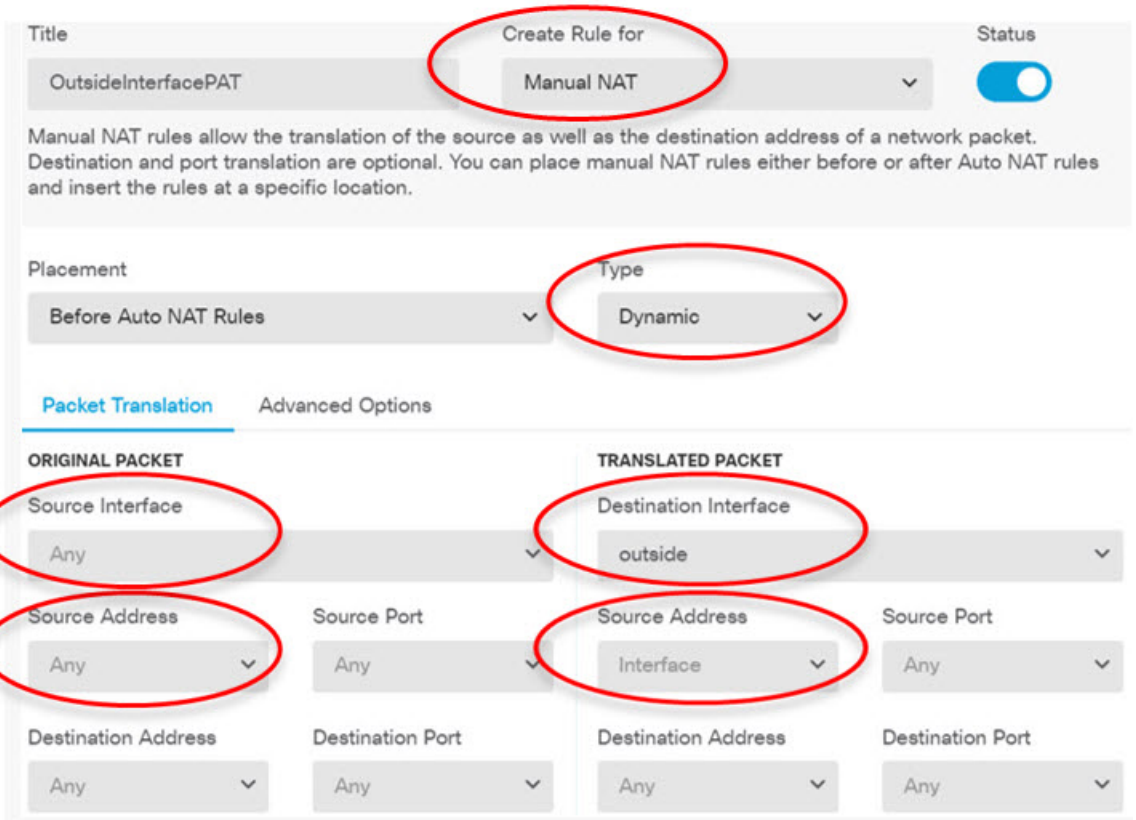
c) 次のプロパティを使用してルールを設定します。

- [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）]。
- [元のパケット（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。[元のパケット（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。

- [変換後のパケット（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。[変換後のパケット（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。

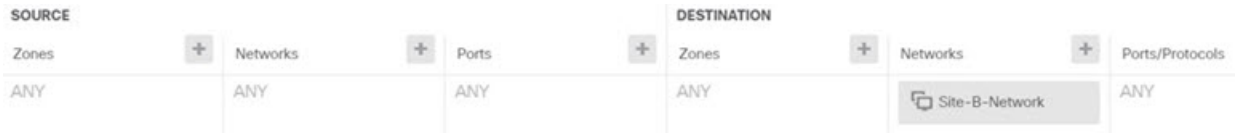
VPN 接続を作成するだけで、VPN 上のトラフィックが自動的に許可されるわけではありません。使用しているアクセス コントロール ポリシーがリモート ネットワークへのトラフィックを許可している必要があります。

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。



- [アプリケーション（Application）]、[URL]、および [ユーザ（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。

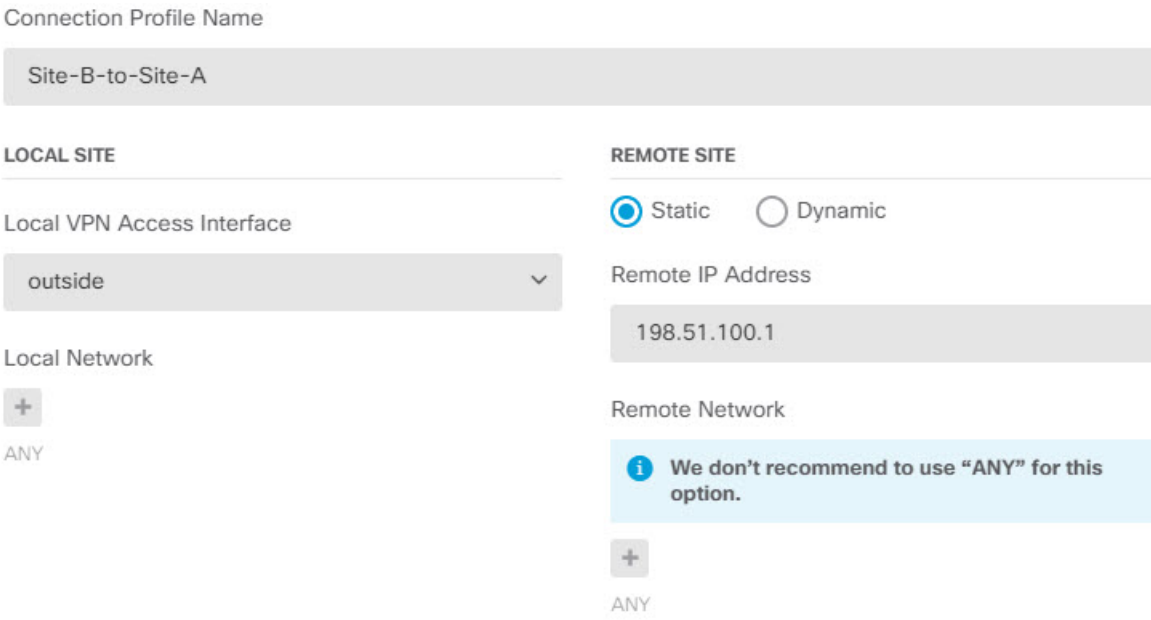
ステップ 5 （サイト B、リモート サイト）リモート サイトのデバイスにログインし、サイト A へのサイト間 VPN 接続を設定します。

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。

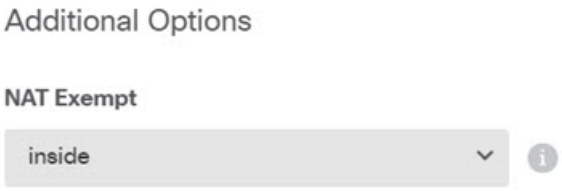
次に、最初の手順の状況を図で示します。



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。



- [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。

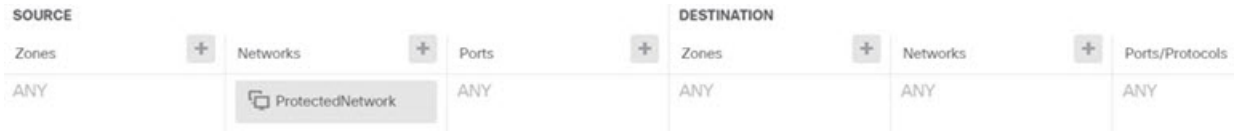
ステップ 7 （サイトB、リモートサイト）保護ネットワークからインターネットへのアクセスを許可するアクセス制御ルールを設定します。

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、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。

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、[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。