Security Cloud Control での仮想プライベートネットワークの管理

バーチャルプライベートネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介してエンドポイント間の安全なトンネルを確立します。

この項の内容は、FDM 管理対象デバイスのリモートアクセスおよびサイト間 VPN に当てはまります。FTD でサイト間 VPN 接続を構築するためのインターネット プロトコル セキュリティ（IPsec）標準について説明しています。また、FTD で VPN 接続を構築し、リモートでアクセスするために使用する SSL 標準についても説明します。

Security Cloud Control は以下のタイプの VPN 接続をサポートしています。

サイト間仮想プライベートネットワークの概要

サイト間 VPN トンネルは、地理的に異なる場所にあるネットワークを接続します。管理対象デバイス間、および管理対象デバイスと関連するすべての規格に準拠するその他のシスコまたはサードパーティのピアとの間で、サイト間 IPsec 接続を作成できます。これらのピアは、IPv4 アドレスと IPv6 アドレスの内部と外部の任意の組み合わせを持つことができます。サイト間トンネルは、Internet Protocol Security（IPsec）プロトコルスイートとインターネット キー エクスチェンジ バージョン 2（IKEv2）を使用して構築されます。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな 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に接続することができます。

Security Cloud Control を使用したサイト間 VPN の簡素化

サイト間 VPN は、インターネット上で複数のネットワークを安全に接続するための信頼性の高いソリューションです。このプロセスをより簡単かつ効率的に行うために、Security Cloud Control では**統合されたサイト間 VPN ウィザード**が提供されています。この直感的なツール

は、従来の VPN 設定に伴う複雑さを軽減しながら、セキュアな VPN トンネルの作成と管理を簡素化するように設計されています。

サイト間 VPN ウィザードは、さまざまな管理対象デバイス間で VPN トンネルを設定するための単一の統合インターフェイスを提供します。この一貫性により、特定のデバイスやネットワーク環境に関係なく、管理者のエクスペリエンスは合理化されます。ウィザードは、一元化された直感的な設定プロセスを提供することで、組織のネットワークインフラストラクチャにおける運用効率の向上、エラーの減少、高レベルのセキュリティの維持を支援します。

次の表に、管理対象デバイスで許可されているサイト間 VPN 設定を示します。

	FDM-managed	Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense	Secure Firewall ASA	Multicloud Defense
FDM-managed	対応	非対応	非対応	非対応
Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense	非対応	対応	対応	対応
Secure Firewall ASA	非対応	対応	対応	対応
Multicloud Defense	非対応	対応	対応	非対応

サイト間 VPN の概念

VPN トポロジ

新しいサイト間VPNトポロジを作成するには、一意の名前を付け、トポロジタイプを指定し、IPsec IKEv1 または IKEv2 あるいはその両方に使用される IKE バージョンと認証方式を選択する必要があります。設定したら、FTD にトポロジを展開します。

IPsec および IKE プロトコル

Security Cloud Control では、サイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよび IPsec プロポーザルに基づいて設定されます。ポリシーとプロポーザルはパラメータのセットであり、これらのパラメータによって、IPsec トンネル内のトラフィックでセキュリティを確保するために使用されるセキュリティ プロトコルやアルゴリズムなど、サイト間 VPN の特性が定義されます。VPN トポロジに割り当て可能な完全な設定イメージを定義するために、複数のポリシー タイプが必要となる場合があります。

認証 VPN トンネル

VPN接続の認証には、各デバイスのトポロジ内で事前共有キーを設定します。事前共有キーにより、IKE 認証フェーズで使用する秘密鍵を 2 つのピア間で共有できます。

バーチャル トンネル インターフェイス（VTI）

現在のところ、Security Cloud Control では FTD の仮想トンネルインターフェイス（VTI）のトンネルを管理、モニタリング、使用できません。VTI トンネルが設定されているデバイスを Security Cloud Control にオンボーディングすることは可能ですが、VTI インターフェイスは無視されます。セキュリティゾーンまたはスタティックルートが VTI を参照する場合、Security Cloud Control は VTI 参照を除いてセキュリティゾーンとスタティックルートを読み取ります。

VPN 暗号化ドメイン

VPNの暗号化ドメインを定義するには、ルートベースまたはポリシーベースのトラフィックセレクタの 2 つの方法があります。

- **ポリシーベース**：暗号化ドメインは、IPSec トンネルに入るすべてのトラフィックを許可するように設定されます。IPSec ローカルおよびリモートのトラフィックセレクタは0.0.0.0に設定されます。これは、IPSec トンネルにルーティングされるトラフィックはすべて、送信元/接続先のサブネットに関係なく暗号化されることを意味します。ASAは、暗号マップを使用したポリシーベースの VPN をサポートします。
- **ルートベース**： 暗号化ドメインは、送信元と接続先の両方が特定の IP 範囲にある場合のみ暗号化するように設定されます。仮想IPsecインターフェイスが作成され、そのインターフェイスに入るトラフィックはすべて暗号化および復号されます。ASAは、仮想トンネルインターフェイス（VTI）を使用してルートベースの VPN をサポートします。

エクストラネットデバイスについて

シスコ製以外のデバイスまたは管理対象外のシスコデバイスを、静的 IP アドレスまたは動的 IP アドレスのいずれかを使用して「エクストラネット」デバイスとして VPN トポロジに追加できます。

- シスコ製以外のデバイス：Security Cloud Control を使用して、シスコ製以外のデバイスに対する設定を作成したり、展開したりすることはできません。
- 管理対象外のシスコデバイス：組織によって管理されないシスコデバイス。たとえば、社内の他の部門が管理するネットワーク内のスポークや、サービスプロバイダーまたはパートナーネットワークへの接続などです。

グローバル IKE ポリシーについて

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行するかを決定します。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。

次に、各バージョンの IKE ポリシーの設定方法を説明します。

- IKEv1 ポリシーの設定
- IKEv2 ポリシーの設定

IKEv1 ポリシーの管理

IKEv1 ポリシーについて

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。

関連トピック

IKEv1 ポリシーの作成 （5 ページ）

IKEv1 ポリシーの作成

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。サイト間 VPN 接続での IKE 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IKEv1 ポリシーの作成（Create New IKEv1 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 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで [オブジェクト（Objects）] をクリックします。

ステップ 3 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、**[FDM]** > **[IKEv1 ポリシー（IKEv1 Policy）]** を選択して、新しい IKEv1 ポリシーを作成します。
- オブジェクトのページで、編集する IKEv1 ポリシーを選択し、右側の [操作（Actions）] ウィンドウで [編集（Edit）] をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を 128 文字以内で入力します。

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順位（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。
- [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」を参照してください。
- [Diffie-Hellmanグループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密を互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほど

セキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。オプションの説明については、「使用する Diffie-Hellman 係数グループの決定」を参照してください。

- [ライフタイム（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）。
- [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」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。
- [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」を参照してください。

ステップ 6 [Add] をクリックします。

IKEv2 ポリシーの管理

IKEv2 ポリシーについて

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。

関連トピック

IKEv2 ポリシーの作成 （7 ページ）

IKEv2 ポリシーの作成

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。サイト間 VPN 接続での IKE 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IKEv2ポリシーの作成（Create New IKEv2 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 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで [オブジェクト（Objects）] をクリックします。

ステップ 3 次のいずれかの操作を実行します。

- 青色のプラスボタン  をクリックし、**[FDM]** > **[IKEv2ポリシー（IKEv2 Policy）]** を選択して、新しい IKEv2 ポリシーを作成します。
- オブジェクトページで、編集する IKEv2 ポリシーを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を 128 文字以内で入力します。

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順位（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。

- [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（通常モードでは整合性ハッシュを選択する必要がありますが、混合モードでは個別の整合性ハッシュの選択は禁止されています）。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」を参照してください。
- [Diffie-Hellman グループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密を互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。許可する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」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」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）]：ハッシュアルゴリズムの疑似ランダム関数（PRF）部分。このアルゴリズムは IKEv2 トンネル暗号化に必要なキー関連情報とハッシュ操作を取得するために使用されます。IKEv1 では、整合性と PRF アルゴリズムは別ですが、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」を参照してください。
- [ライフタイム（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 [Add] をクリックします。

IPsec プロポーザルについて

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 IPSec プロポーザルオブジェクトの作成および編集
- IKEv2 IPSec プロポーザルオブジェクトの作成および編集

IPsec プロポーザルオブジェクトの管理

IPsec プロポーザル オブジェクトは、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。IKEv1 と IKEv2 に対して、異なるオブジェクトがあります。現在、Security Cloud Control は IKEv1 IPsec プロポーザルオブジェクトをサポートしています。

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。このプロトコルにより、認証、暗号化、およびアンチリプレイサービスが実現します。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。

関連トピック

IKEv1 IPsec プロポーザルオブジェクトの作成 （10 ページ）

IKEv1 IPsec プロポーザルオブジェクトの作成

IPsec プロポーザル オブジェクトは、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。IKEv1 と IKEv2 に対して、異なるオブジェクトがあります。現在、Security Cloud Control は IKEv1 IPsec プロポーザルオブジェクトをサポートしています。

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。このプロトコルにより、認証、暗号化、およびアンチリプレイサービスが実現します。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。

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。サイト間 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IKEv1プロポーザルの作成（Create New IKEv1 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 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Objects** をクリックします。

ステップ 3 次のいずれかの操作を実行します。

- 青色のプラスボタン をクリックし、**[FTD]** > **[IKEv1 IPSecプロポーザル（IKEv1 IPsec Proposal）]** を選択して新しいオブジェクトを作成します。

- オブジェクトページで、編集する IPSec プロポーザルを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 4 新しいオブジェクトのオブジェクト名を入力します。

ステップ 5 IKEv1 IPSec プロポーザルオブジェクトが動作するモードを選択します。

- トンネルモードでは IP パケット全体がカプセル化されます。IPSec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これがデフォルトです。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。
- トランスポートモードでは IP パケットの上位層プロトコルだけがカプセル化されます。IPSec ヘッダーは、IP ヘッダーと上位層プロトコル ヘッダー（TCP など）との間に挿入されます。トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポート モードは、レイヤ 2 またはレイヤ 3 のトンネリング プロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。

ステップ 6 このプロポーザルの [ESP暗号化（ESP Encryption）]（カプセル化セキュリティプロトコル暗号化）アルゴリズムを選択します。詳細については、「使用する暗号化アルゴリズムの決定」を参照してください。

ステップ 7 認証に使用する [ESPハッシュ（ESP Hash）] または整合性アルゴリズムを選択します。詳細については、「使用するハッシュアルゴリズムの決定」を参照してください。

ステップ 8 [Add] をクリックします。

IKEv2 IPsec プロポーザルオブジェクトの管理

IPsec プロポーザル オブジェクトは、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。

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。

関連トピック

IKEv2 IPSec プロポーザルオブジェクトの作成または編集 （12 ページ）

IKEv2 IPSec プロポーザルオブジェクトの作成または編集

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 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Objects** をクリックします。

ステップ 3 次のいずれかの操作を実行します。

- 青色のプラスボタン をクリックし、**[FTD]** > **[IKEv2 IPsecプロポーザル（IKEv2 IPsec Proposal）]** を選択して新しいオブジェクトを作成します。
- オブジェクトページで、編集する IPSec プロポーザルを選択し、右側の [アクション（Actions）] ペインで [編集（Edit）] をクリックします。

ステップ 4 新しいオブジェクトのオブジェクト名を入力します。

ステップ 5 IKEv2 IPsec プロポーザルオブジェクトの設定：

- [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」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」を参照してください。

ステップ 6 [Add] をクリックします。

VPN で使用される暗号化アルゴリズムとハッシュアルゴリズム

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 プロポーザルに対して使用する暗号化アルゴリズムを決定する場合は、VPN 内のデバイスによってサポートされるアルゴリズムに限定されます。

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、アルゴリズム名の接頭辞が「ESP」となります。

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）ガロア/カウンタモードの Advanced Encryption Standard は、機密性とデータ発信元認証を提供するブロック暗号モードの操作であり、AES より優れたセキュリティを実現します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。GCM は NSA Suite B をサポートするために必要となる 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、計算の効率は 3DES よりも高いです。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（Data Encryption Standard）は、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。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、安全性は劣ります。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。
- 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。
- 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、アルゴリズム名の接頭辞が「ESP-」となり、「-HMAC」（Hash Method Authentication Code）という接尾辞も使用されます。

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。

次のハッシュ アルゴリズムから選択できます。

- [SHA (Secure Hash Algorithm)]：標準の SHA（SHA-1）は、160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。ただし、MD5 よりも多くのリソースを消費します。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。
- 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。

- 2：Diffie-Hellman グループ 2（1024 ビット Modular Exponential（MODP）グループ）。このオプションは十分な保護レベル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 ビットキーの十分な保護レベルと見なされていましたが、このオプションは十分な保護レベルとは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 グループと 256 ビット素数位数部分群）。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。

FDM-Managed のサイト間 VPN 設定

Security Cloud Control は、FDM-managed デバイスの備えるサイト間 VPN 機能の次の側面をサポートしています。

- IPsec IKEv1 および IKEv2 プロトコルの両方をサポート。
- 自動または手動の事前共有認証キー。
- IPv4 および IPv6 内部、外部のすべての組み合わせをサポート。
- IPsec IKEv2 サイト間 VPN トポロジにより、セキュリティ認定に準拠するための設定を提供。
- スタティック インターフェイスおよびダイナミック インターフェイス。
- エクストラネットデバイスのダイナミック IP アドレスをエンドポイントとしてサポート。

動的にアドレス指定されたピアによるサイト間 VPN 接続の設定

Security Cloud Control を使用すると、ピアのいずれかの VPN インターフェイス IP アドレスが不明な場合、またはインターフェイスが DHCP サーバーからアドレスを取得する場合に、ピア間にサイト間 VPN 接続を作成できます。事前共有キー、IKE 設定、および IPsec 設定が別のピアと一致するダイナミックピアは、サイト間 VPN 接続を確立できます。

A と B の 2 つのピアがあるとします。スタティックピアは、VPN インターフェイスの IP アドレスが固定されているデバイスであり、ダイナミックピアは、VPN インターフェイスの IP アドレスが不明であるか、一時的な IP アドレスを持つデバイスです。

次の使用例では、動的にアドレス指定されたピアとの安全なサイト間 VPN 接続を確立するためのさまざまなシナリオについて説明します。

- A はスタティックピア、B はダイナミックピア、またはその逆です。

- A はスタティックピア、B は DHCP サーバーから解決された IP アドレスを持つダイナミックピア、またはその逆です。[VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択して、スタティックピアの IP アドレスと、ダイナミックピアの DHCP によって割り当てられた IP アドレスの間に VPN 接続を確立できます。
- A と B はダイナミックピアであり、DHCP サーバーからの解決済み IP アドレスを使用します。このような場合、スタティックピアの IP アドレスと、ダイナミックピアの DHCP によって割り当てられた IP アドレスとの間に VPN 接続を確立するために、少なくとも 1 つのピアに対して [VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択する必要があります。
- A はダイナミックピアで、B はスタティックまたはダイナミック IP アドレスを持つエクストラネットデバイスです。
- A は DHCP サーバーからの解決済み IP アドレスを持つダイナミックピアで、B はスタティックまたはダイナミック IP アドレスを持つエクストラネットデバイスです。[VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択して、スタティックピアの IP アドレスと、ダイナミックピアの DHCP によって割り当てられた IP アドレスの間に VPN 接続を確立できます。

重要 [VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択すると、VPN は DHCP によって割り当てられた IP アドレスに静的にバインドします。ただし、このダイナミックインターフェイスは、ピアの再起動後に多くの新しい IP アドレスを受信できます。VPN トンネルは新しい IP アドレスを更新しますが、もう一方のピアは新しい設定で更新されません。他のピアでのアウトオブバンドの変更については、サイト間設定を再度展開する必要があります。

（注） Firewall Device Manager などのローカルマネージャを使用してインターフェイスの IP アドレスを変更すると、Security Cloud Control では、そのピアの [設定ステータス（Configuration Status）] に [競合検出（Conflict Detected）] と表示されます。このアウトオブバンドの変更を解決すると、他方のピアの [設定ステータス（Configuration Status）] が [未同期（Not Synced）] 状態に変わります。[未同期（Not Synced）] 状態のデバイスに Security Cloud Control 設定を展開する必要があります。

通常、ダイナミックピアの IP アドレスを他方のピアは把握していないため、ダイナミックピアから接続を開始する必要があります。リモートピアが接続を確立しようとすると、他方のピアは事前共有キー、IKE 設定、および IPsec 設定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。

（注） 次のシナリオでは、サイト間 VPN 接続を設定できません。

- 両方のピアに DHCP によって割り当てられた IP アドレスがある場合。
  - **回避策**：どちらか一方のピアに DHCP サーバーからの解決済み IP アドレスがある場合は、サイト間 VPN を設定できます。このような場合、サイト間 VPN を設定するには [VPNを割り当てられたIPにバインドする（Bind VPN to the assigned IP）] を選択する必要があります。
- 1 台のデバイスに複数のダイナミックピア接続がある場合。
  - **回避策**：次の手順を実行して、サイト間 VPN を設定できます。
    - 3 台のデバイス A、B、C があるとします。
    - A（スタティックピア）と B（ダイナミックピア）間のサイト間 VPN 接続を設定します。
    - エクストラネットデバイスを作成して、A と C（ダイナミックピア）間のサイト間 VPN 接続を設定します。A のスタティック VPN インターフェイス IP アドレスをエクストラネットデバイスに割り当て、C との接続を確立します。

FDM-Managed デバイスのサイト間 VPN ガイドラインと制約事項

- Security Cloud Control は、S2S VPN の対象トラフィックを設計するための crypto-acl をサポートしていません。保護されたネットワークのみをサポートします。
- Security Cloud Control は、現在、ASA デバイスまたは FDM-managed デバイス上の仮想トンネルインターフェイス（VTI）トンネルの管理、監視、使用をサポートしていません。VTI トンネルが設定されているデバイスを Security Cloud Control にオンボーディングすることは可能ですが、VTIインターフェイスは無視されます。セキュリティゾーンまたはスタティックルートが VTI を参照する場合、Security Cloud Control は VTI 参照を除いてセキュリティゾーンとスタティックルートを読み取ります。VTI トンネルに対する Security Cloud Control のサポートは近日中に提供されます。
- IKE ポート 500/4500 が使用されている場合、またはアクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、サイト間 VPN を同じポートに設定することはできません。
- トンネルモードにのみ対応し、トランスポートモードには対応していません。IPsec トンネル モードは、新しい IP パケットのペイロードになる元の IP データグラム全体を暗号化します。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。

- このリリースでは、1 つ以上の VPN トンネルを含む PTP トポロジのみがサポートされています。ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。

FDM-managed デバイス間のサイト間 VPN トンネルの作成

FDM-managed デバイスは、別の FDM-managed デバイスまたはエクストラネットデバイスとの間にセキュアな VPN トンネルを確立できることに注意してください。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** を選択します。

ステップ 3 [トンネルの作成（Create Tunnel）]（  ）アイコンをクリックし、[サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 4 [ピアの選択（Peer Selection）] エリアで、次の情報を入力します。

- [設定名（Configuration Name）]：一意のトポロジ名を入力します。

  トポロジには、FDM-managed デバイス VPN であることとトポロジタイプを示す名前を付けることをお勧めします。

- [ピア1（Peer 1）]：[FDM] タブをクリックして、FDM-managedデバイスを選択します。

- [ピア2（Peer 2）]：[FDM] タブをクリックして、FDM-managedデバイスを選択します。

  エクストラネットデバイスを選択する場合は、[静的（Static）] を選択して IP アドレスを指定し、DHCP が割り当てられた IP を持つエクストラネットデバイスの場合は [動的（Dynamic）] を選択します。[IPアドレス（IP Address）] には、静的インターフェイスの IP アドレスまたは動的インターフェイスの [DHCP割り当て（DHCP Assigned）] が表示されます。

  （注）
  1 つまたは両方のエンドポイントデバイスに動的 IP アドレスがある場合、追加の手順については、「動的にアドレス指定されたピアを使用したサイト間 VPN 接続の設定」を参照してください。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ピアの詳細（Peer Details）] エリアで、次の情報を入力します。

- [VPNアクセスインターフェイス（VPN Access Interface）]：ピア 1 とピア 2 間の接続を確立するインターフェイスを選択します。

- [ルーティング（Routing）]：[ネットワークの追加（Add Networks）] をクリックし、1 つ以上の保護されたネットワークを選択して、ピア 1 とピア 2 の保護されたネットワークの間にサイト間トンネルを作成します

- （オプション）[NAT免除インターフェイス（NAT Exempt Interface）]：ピア 1 とピア 2 について [NAT免除（NAT Exempt）] を選択し、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 ポリシーから除外します。個々のピアに対して手動で設定する必要があります。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。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [IKE設定（IKE Settings）] エリアで、インターネット キー エクスチェンジ（IKE）のネゴシエーション中に使用する IKE バージョンを選択し、プライバシー設定を指定します。IKE ポリシーの詳細については、「グローバル IKE ポリシーの設定」を参照してください。

（注）
IKE ポリシーはデバイスに対してグローバルであり、デバイスに関連付けられたすべての VPN トンネルに適用されます。したがって、ポリシーを追加または削除すると、このデバイスが参加しているすべての VPN トンネルに影響します。

1. 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。

   （注）
   デフォルトでは、[IKEVバージョン2] が有効になっています。

2. [IKEv2ポリシーの追加（Add IKEv2 Policies）] をクリックし、ピア 1 とピア 2 の IKEv2 ポリシーを選択します。
3. 参加デバイスの [ローカル事前共有キー（Local Pre-Shared Key）] と [リモート事前共有キー（Remote Pre-Shared Key）] が自動生成されます。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。
4. [IKEバージョン1（IKE Version 1）] をクリックして有効にします。
5. [IKEv1ポリシーの追加（Add IKEv1 Policies）] をクリックし、ピア 1 とピア 2 の IKEv1 ポリシーを選択します。
6. [IPEv1事前共有キー（IPEv1 Pre-Shared Key）] が自動生成されます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [IPSec設定（IPSec Settings）] エリアで、ピア 1 およびピア 2 の IPSec 設定を指定します。[IPSec設定（IPSec Settings）] ステップでの選択に応じて、対応する IKEv プロポーザルを使用できます。

IPSec 設定の詳細については、「IPsec プロポーザルについて」を参照してください。

1. [IKEv2 IPSecプロポーザルの追加（Add IKEv2 IPSec Proposals）] をクリックし、ピア 1 とピア 2 に使用する IKEv2 プロポーザルを選択します。

2. [Perfect Forward Secrecy対応のDiffie-Hellmanグループ（Diffie-Hellman Group for Perfect Forward Secrecy）] を選択します。詳細については、「使用する Diffie-Hellman 係数グループの決定」を参照してください。
3. [次へ（Next）] をクリックします。

ステップ 11 [終了（Finish）] エリアに、完了した構成の概要が表示されます。

設定を確認し、問題がなければ [送信（Submit）] をクリックします。

サイト間ピア間の保護されたトラフィックのネットワークの設定

サイト間接続の設定が完了したら、VPN がすべての対象デバイスで機能するように、次の設定を実行してください。

手順

ステップ 1 AC ポリシーを設定します。

両方のピアの背後にある保護されたネットワーク間の双方向トラフィックを許可するための AC ポリシーを設定します。AC ポリシーは、パケットがドロップされることなく目的の宛先に到達するのに役立ちます。

（注）
両方のピアで着信トラフィックと発信トラフィックの AC ポリシーを作成する必要があります。

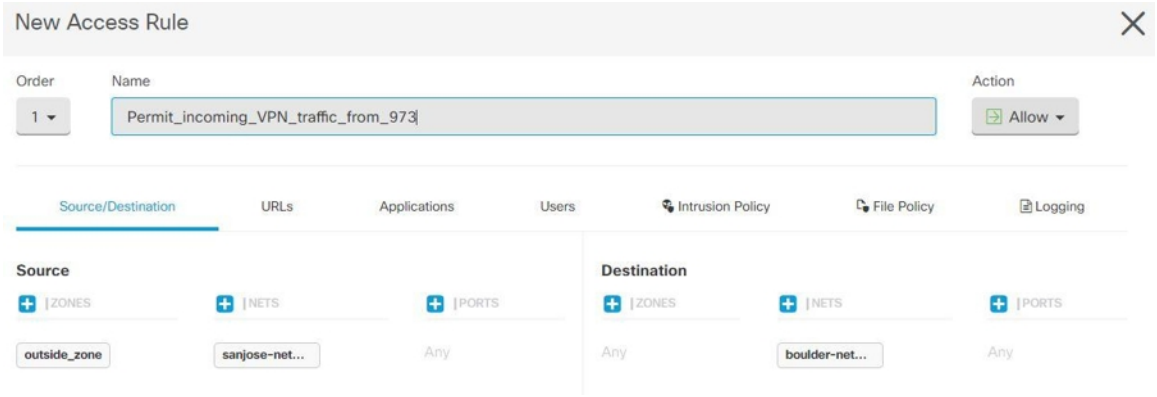
1. 左側の Security Cloud Control ナビゲーションバーで [ポリシー（Policies）] をクリックし、必要なオプションを選択します。
2. 両方のピアで着信トラフィックと発信トラフィックのポリシーを作成します。

   次の例は、両方のピアで AC ポリシーを作成する手順を示しています。

   それぞれ 2 つの保護されたネットワーク「boulder-network」および「sanjose-network」間のサイト間 VPN 接続を備えた 2 つの FDM-managed デバイス「FTD_BGL_972」および「FTD_BGL_973」について考えてみます。

   着信トラフィックを許可する *AC* ポリシーの作成：

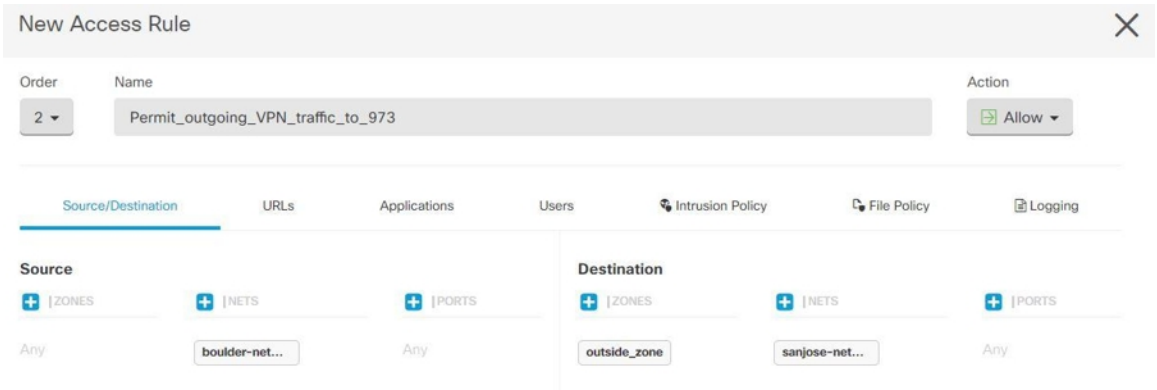
   ポリシー「Permit_incoming_VPN_traffic_from_973」は、ピア「FTD_BGL_973」からの着信トラフィックを許可するために「FTD_BGL_972」デバイスで作成されます。



- **送信元ゾーン**：ネットワークトラフィックの発信元であるピアデバイスのゾーンを設定します。この例では、トラフィックはFTD_BGL_973から発信され、FTD_BGL_972に到達します。
- **送信元ネットワーク**：ネットワークトラフィックの発信元であるピアデバイスの保護されたネットワークを設定します。この例では、トラフィックはピアデバイス（FTD_BGL_973）の背後にある保護されたネットワークである「sanjose-network」から発信されています。
- **宛先ネットワーク**：ネットワークトラフィックが到着するデバイスの保護されたネットワークを設定します。この例では、トラフィックはピアデバイス（FTD_BGL_972）の背後にある保護されたネットワークである「boulder-network」に到着しています。
  注：残りのフィールドは、デフォルト値（「Any」）にできます。
- ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可するには、[アクション（Action）] を [許可（Allow）] に設定します。

発信トラフィックを許可する *AC* ポリシーの作成：

ポリシー「Permit_outgoing_VPN_traffic_to_973」は、ピア「FTD_BGL_973」への発信トラフィックを許可するために「FTD_BGL_972」デバイスで作成されます。



- **送信元ネットワーク**：ネットワークトラフィックの発信元であるピアデバイスの保護されたネットワークを設定します。この例では、トラフィックはピアデバイス

（FTD_BGL_972）の背後にある保護されたネットワークである「boulder-network」から発信されています。

- **宛先ゾーン**：ネットワークトラフィックが到着するピアデバイスのゾーンを設定します。この例では、トラフィックは FTD_BGL_972 から着信し、FTD_BGL_973 に到達しています。
- **宛先ネットワーク**：ネットワークトラフィックが到着するピアの保護されたネットワークを設定します。この例では、トラフィックはピアデバイス（FTD_BGL_972）の背後にある保護されたネットワークである「sanjose-network」に到着しています。**注**：残りのフィールドは、デフォルト値（「Any」）にできます。
- ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可するには、[アクション（Action）] を [許可（Allow）] に設定します。

1 つのデバイスで AC ポリシーを作成したら、そのデバイスのピアで同様のポリシーを作成する必要があります。

ステップ 2 いずれかのピアデバイスで NAT が設定されている場合は、NAT 免除ルールを手動で設定する必要があります。「NAT からのサイト間 VPN トラフィックの除外」を参照してください。

ステップ 3 各ピアでリターン VPN トラフィックを受信するためのルーティングを設定します。

詳細については、「ルーティングの設定」を参照してください。

1. [ゲートウェイ（Gateway）]：宛先ネットワークへのゲートウェイの IP アドレスを識別するネットワークオブジェクトを選択します。トラフィックはこのアドレスに送信されます。
2. [インターフェイス（Interface）]：トラフィックの送信経路となるインターフェイスを選択します。この例では、トラフィックは「外部」インターフェースを介して送信されます。
3. [宛先ネットワーク（Destination Networks）]：宛先ネットワークを識別する 1 つまたは複数のネットワークオブジェクトを選択します。この例では、宛先はピア（FTD_BGL_973）の背後にある「sanjose-network」です。

1 つのデバイスでルーティングの設定をしたら、そのデバイスのピアで同様の設定をする必要があります。

既存の Security Cloud Control サイト間 VPN の編集

高度な設定ウィザードは、デフォルトで既存のサイト間 VPN 設定を変更するために使用します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** を選択します。

ステップ 3 編集するサイト間 VPN トンネルを選択します。

ステップ 4 [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。

（注）
または、次を実行して設定を編集することもできます。

1. VPN ページを開き、[フィルタ（filter）] パネルの [グローバルビュー（Global View）] ボタンをクリックします。（詳細については、「グローバルビュー」を参照してください）。

   すべてのデバイスで使用可能なすべてのサイト間 VPN トンネルの図が表示されます。

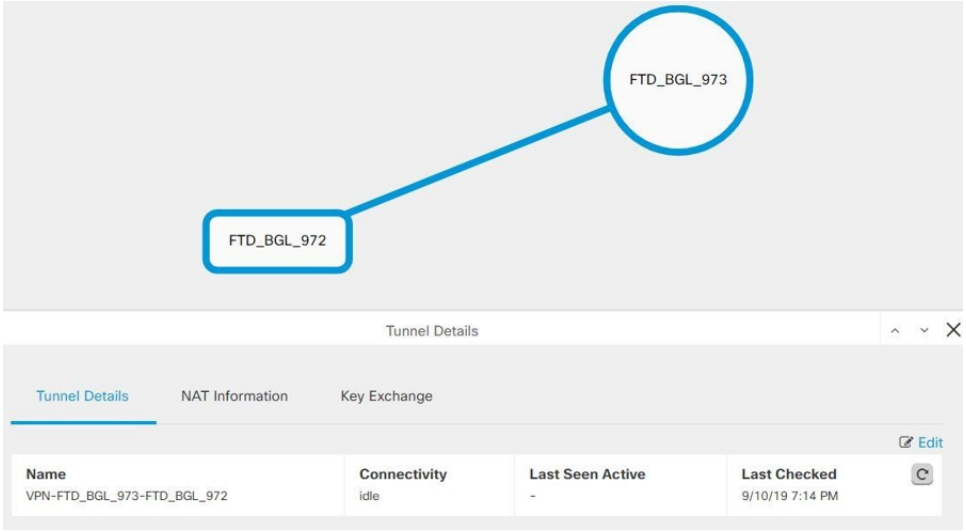
   設定を編集するには、ピアの 1 つが FDM-managed デバイスである必要があります。

2. ボックスをクリックしてデバイスを選択します。

3. ピアを表示するには、[詳細の表示（View Details）] をクリックします。

4. ピアのデバイスをクリックして、トンネルの詳細を表示します。

   トンネルの詳細、NAT 情報、およびデバイスに関するキー交換情報を表示できます。



5. [トンネルの詳細（Tunnel Details）] で [編集（Edit）] をクリックします。

ステップ 5 [ピアデバイス（Peer Devices）] セクションでは、次のデバイス設定を変更できます：設定名、VPN アクセスインターフェイス、および保護されたネットワーク。

（注）
参加デバイスを変更することはできません。

ステップ 6 [IKE 設定（IKE Settings）] セクションでは、次の IKEv2 ポリシー設定を変更できます。

1. それぞれのデバイスの青いプラス ボタンをクリックし、新しい IKEv2 ポリシーを選択します。既存の IKEv2 ポリシーを削除するには、選択したポリシーにカーソルを合わせ、[x] アイコンをクリックします。
2. 参加デバイスの**事前共有キー**を変更します。エンドポイントデバイスの事前共有キーが異なる場合は、青い設定 ボタンをクリックして、デバイスの適切な事前共有キーを入力します。
3. [次へ（Next）] をクリックします。

ステップ 7 [IPSec設定（IPSec Settings）] セクションでは、次の IPSec 設定を変更できます。

1. 青いプラス ボタンをクリックして、新しい IKEv2 プロポーザルを選択します。既存の IKEv2 プロポーザルを削除するには、選択したプロポーザルにカーソルを合わせ、[x] アイコンをクリックします。
2. [Perfect Forward Secrecy対応のDiffie-Hellmanグループ（Diffie-Hellman Group for Perfect Forward Secrecy）] を選択します。
3. [VPN の編集（Edit VPN）] をクリックし、[完了（Finish）] をクリックします。

ポイントツーポイントの VPN が変更され、行ったすべての変更が反映されます。

Security Cloud Control サイト間 VPN トンネルの削除

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。
ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして [VPN] ページを開きます。
ステップ 3 削除するサイト間 VPN トンネルを選択します。
ステップ 4 右側の [アクション（Actions）] ペインで、[削除（Delete）] をクリックします。

選択したサイト間 VPN トンネルが削除されます。

NAT からのサイト間 VPN トラフィックの除外

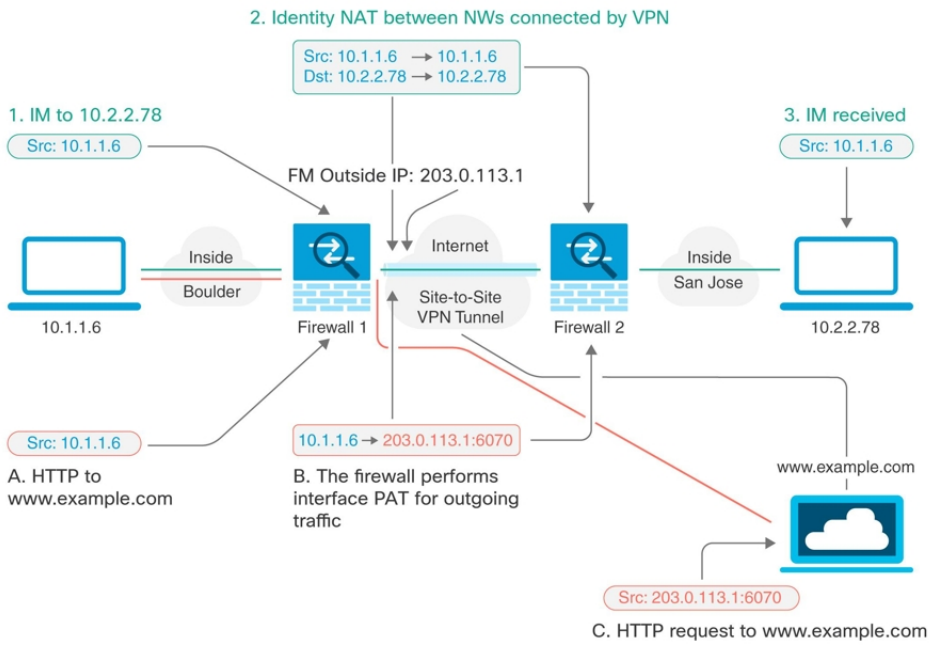
インターフェイスでサイト間 VPN 接続が定義されていて、かつそのインターフェイス向けの NAT ルールを指定している場合、NAT ルールから VPN 上のトラフィックを任意で除外できます。この操作は、VPN 接続のリモート エンドが内部アドレスを処理できる場合に行うと便利です。

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 ポート アドレス変換（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。



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。

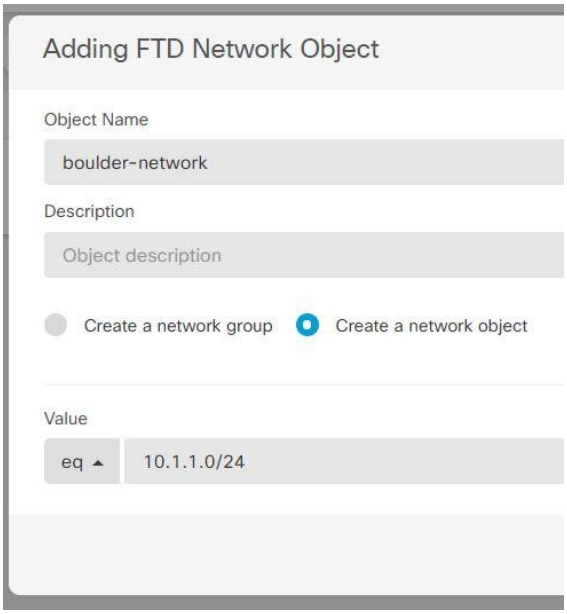
手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 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。

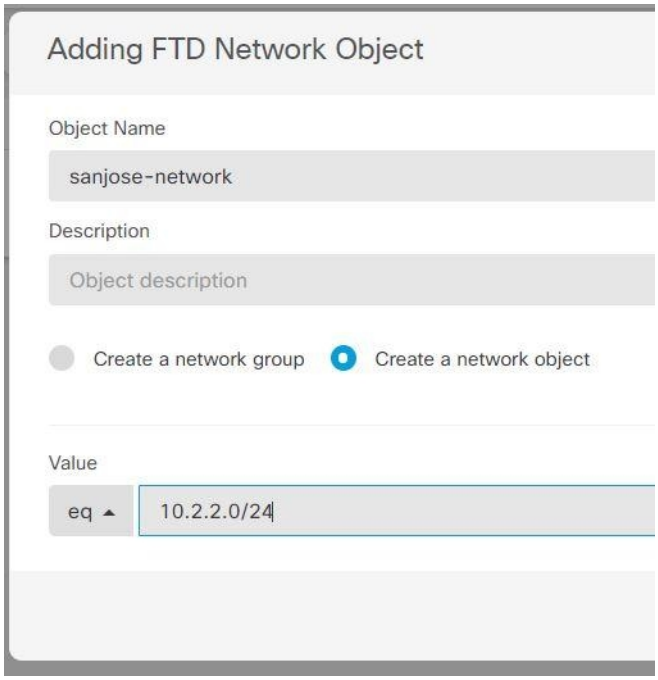
1. 左側のペインで [オブジェクト（Objects）] をクリックします。
2. 青色のプラスボタン をクリックして、オブジェクトを作成します。
3. **[FTD]** > **[ネットワーク（Network）]** をクリックします。
4. ネットワーク内でボールダーを特定します。
5. オブジェクト名を入力します（例：boulder-network）。
6. [ネットワークオブジェクトの作成（Create a network object）] を選択します。
7. [値（Value）] セクションで、次の手順を実行します。
   - [eq] を選択して、単一の IP アドレスまたは CIDR 表記で表されるサブネットアドレスを入力します。

- [範囲（range）] を選択し、IP アドレスの範囲を入力します。たとえば、ネットワークアドレスを 10.1.1.0/24 と入力します。



8. [追加（Add）] をクリックします。
9. 青色のプラスボタン をクリックして、オブジェクトを作成します。
10. サンノゼの内部ネットワークを定義します。
11. オブジェクト名を入力します（例：san-jose）。
12. [ネットワークオブジェクトの作成（Create a network object）] を選択します。
13. [値（Value）] セクションで、次の手順を実行します。
    - [eq] を選択して、単一の IP アドレスまたは CIDR 表記で表されるサブネットアドレスを入力します。

- [範囲（range）] を選択し、IP アドレスの範囲を入力します。たとえば、ネットワークアドレスを 10.1.1.0/24 と入力します。

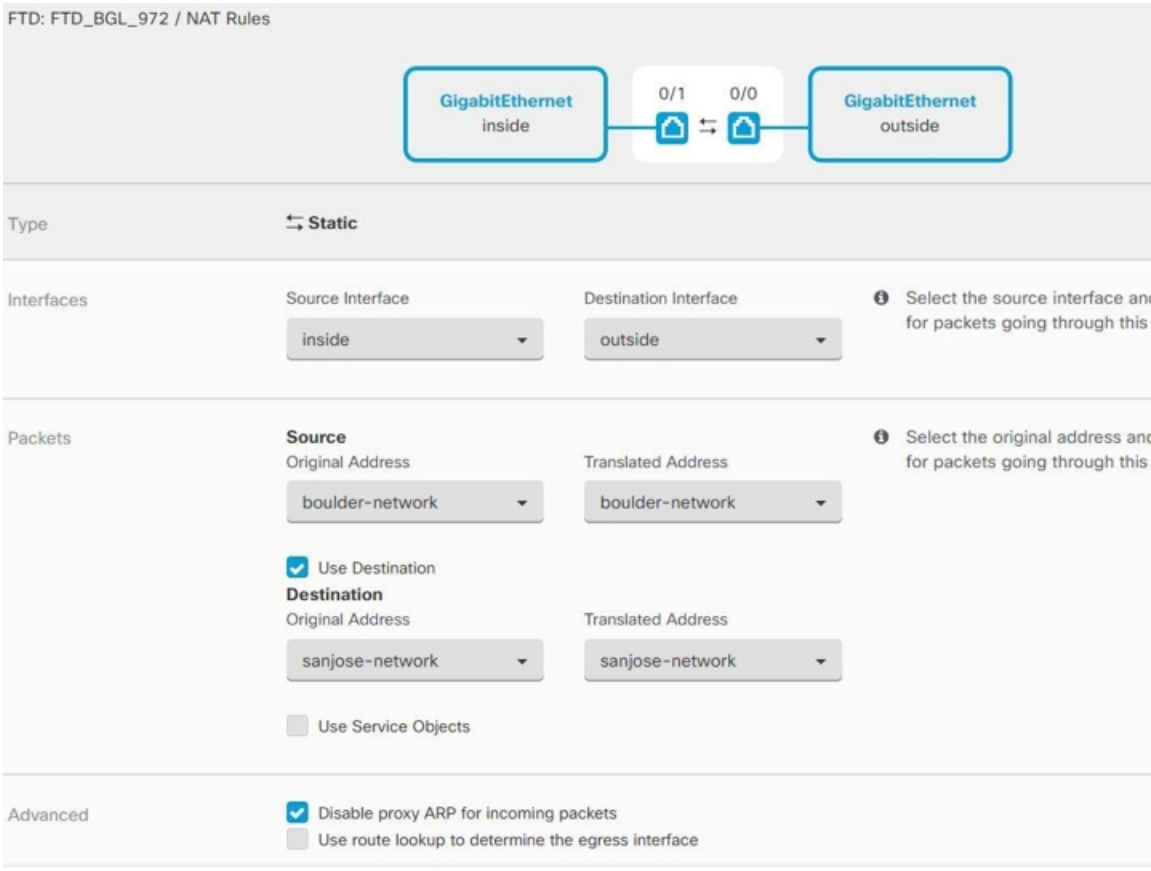


14. [追加（Add）] をクリックします。

ステップ 3 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。

1. 左側のペインで **[セキュリティデバイス（Security Devices）] > [すべてのデバイス（All Devices）]** の順にクリックします。
2. フィルタを使用して、NAT ルールを作成するデバイスを見つけます。
3. 詳細パネルの [管理（Management）] 領域で、[NAT] NAT をクリックします。
4. + > [Twice NAT] をクリックします。
   - セクション 1 で、[静的（Static）] を選択します。 [続行（Continue）] をクリックします。
   - セクション 2 で、[送信元インターフェイス（Source Interface）] = [内部（inside）] および [宛先インターフェイス（Destination Interface）] = [外部（outside）] を選択します。[続行（Continue）] をクリックします。
   - セクション 3 で、[送信元の元のアドレス（Source Original Address）] = 'boulder-network' および [送信元の変換後アドレス（Source Translated Address）] = 'boulder-network' を選択します。
   - [宛先を使用（Use Destination）] を選択します。

- [宛先の元のアドレス（Destination Original Address）] = 'sanjose-network' および [送信元の変換後アドレス（Source Translated Address）] = 'sanjose-network' を選択します。**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。

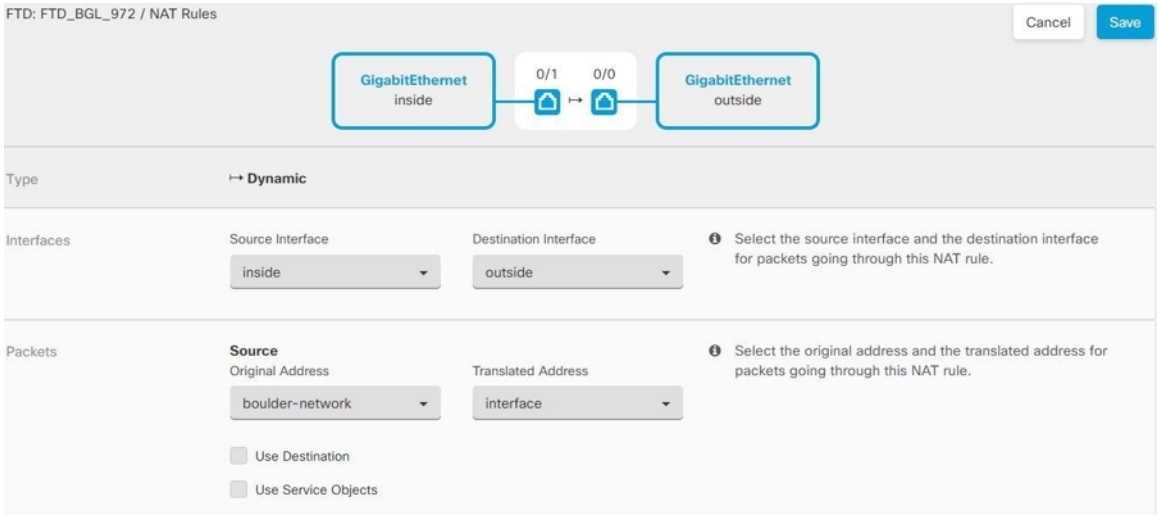


- [着信パケットのプロキシ ARP の無効化（Disable proxy ARP for incoming packets）] を選択します。
- [保存（Save）] をクリックします。
- 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 4 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：IPv4 トラフィックを対象とする内部インターフェイス用ダイナミック インターフェイス PAT ルールは、初期設定時にデフォルトで作成されるので、既に存在する可能性があります。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。

1.  > [Twice NAT] をクリックします。
2. セクション 1 で、[ダイナミック（Dynamic）] を選択します。[続行（Continue）] をクリックします。
3. セクション 2 で、[送信元インターフェイス（Source Interface）] = [内部（inside）] および [宛先インターフェイス（Destination Interface）] = [外部（outside）] を選択します。[続行（Continue）] をクリックします。
4. セクション 3 で、[送信元の元のアドレス（Source Original Address）] = 'boulder-network' および [送信元の変換後アドレス（Source Translated Address）]='インターフェイス（interface）' を選択します。



5. [保存（Save）] をクリックします。
6. 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 5 設定変更を Security Cloud Control に展開します。詳細については、「Security Cloud Control から FTD への設定変更の展開」を参照してください。

ステップ 6 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。

FDM-Managed デバイスのスタティックルートとデフォルトルートの設定

Firepower Threat Defense（FTD）デバイスでスタティックルートを定義して、システムのインターフェイスに直接接続されていないネットワークに向かうパケットの送信先をデバイスが認識できるようにします。

デフォルトルートの作成を検討してください。これは、ネットワーク 0.0.0.0/0 のルートです。このルートは、既存の NAT変換、スタティック NAT ルール、またはその他のスタティックルートでは出力インターフェイスを判別できないパケットの送信先を定義します。

デフォルト ゲートウェイを使用してもすべてのネットワークに到達できない場合、他のスタティック ルートが必要になる可能性があります。たとえば、デフォルト ルートは通常、外部インターフェイスの上流に位置するルータです。デバイスに直接接続されていない追加の内部ネットワークがあり、それらにデフォルト ゲートウェイを介してアクセスできない場合、これらそれぞれの内部ネットワークに対してスタティック ルートが必要です。

システムのインターフェイスに直接接続されたネットワークのスタティック ルートを定義することはできません。システムは自動でこれらのルートを作成します。

Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense のサイト間 VPN 設定

Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense デバイスと次のデバイスとの間にサイト間 IPSec 接続を作成できます。

- Firewall Threat Defense
- Secure Firewall ASA
- Multicloud Defense

Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense デバイス間のサイト間 VPN トンネルの作成

次の手順を使用して、Cloud-Delivered Firewall Management Center によって管理される 2 つの Firewall Threat Defense デバイスの間にサイト間 VPN トンネルを作成します。

始める前に

Firewall Threat Defense デバイスに保留中の展開があってはなりません。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** を選択します。

ステップ 3 [トンネルの作成（Create Tunnel）]（  ）アイコンをクリックし、[サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 4 [ピアの選択（Peer Selection）] エリアで、次の情報を入力します。

- [設定名（Configuration Name）]：一意のトポロジ名を入力します。

  トポロジには、Firewall Threat Defense デバイス VPN であることとトポロジタイプを示す名前を付けることをお勧めします。

- **ピア 1（Peer 1）**：**[FTD]** タブをクリックして、Firewall Threat Defense デバイスを選択します。

- **ピア 2（Peer 2）**：**[FTD]** タブをクリックして、Firewall Threat Defense デバイスを選択します。

  エクストラネットデバイスを選択する場合は、[静的（Static）] を選択して IP アドレスを指定し、DHCP が割り当てられた IP を持つエクストラネットデバイスの場合は [動的（Dynamic）] を選択します。[IPアドレス（IP Address）] には、静的インターフェイスの IP アドレスまたは動的インターフェイスの [DHCP割り当て（DHCP Assigned）] が表示されます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ピアの詳細（Peer Details）] エリアで、次の情報を入力します。

- [VPNアクセスインターフェイス（VPN Access Interface）]：ピア 1 とピア 2 の両方のインターフェイスを選択して、それらの間に接続を確立します。

- **LAN インターフェイス（LAN Interfaces）**：LAN サブネットを制御するピア 1 とピア 2 の両方のインターフェイスを選択します。複数のインターフェイスを選択できます

- [ルーティング（Routing）]：[ネットワークの追加（Add Networks）] をクリックし、ピア 1 とピア 2 に対して 1 つ以上の保護されたネットワークを選択して、それらの間にサイト間トンネルを作成します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [IKE設定（IKE Settings）] エリアで、インターネット キー エクスチェンジ（IKE）のネゴシエーション中に使用する IKE バージョンを選択し、プライバシー設定を指定します。IKE ポリシーの詳細については、「グローバル IKE ポリシーの設定」を参照してください。

（注）
IKE ポリシーはデバイスに対してグローバルであり、デバイスに関連付けられたすべての VPN トンネルに適用されます。したがって、ポリシーを追加または削除すると、このデバイスが参加しているすべての VPN トンネルに影響します。

1. 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。

   （注）
   デフォルトでは、[IKEVバージョン2] が有効になっています。

2. [IKEv2ポリシーの追加（Add IKEv2 Policies）] をクリックし、ピア 1 とピア 2 の IKEv2 ポリシーを選択します。
3. 参加デバイスの [ローカル事前共有キー（Local Pre-Shared Key）] と [リモート事前共有キー（Remote Pre-Shared Key）] が自動生成されます。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。
4. [IKEバージョン1（IKE Version 1）] をクリックして有効にします。
5. [IKEv1ポリシーの追加（Add IKEv1 Policies）] をクリックし、ピア 1 とピア 2 の IKEv1 ポリシーを選択します。
6. [IPEv1事前共有キー（IPEv1 Pre-Shared Key）] が自動生成されます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [IPSec設定（IPSec Settings）] エリアで、ピア 1 およびピア 2 の IPSec 設定を指定します。[IPSec 設定（IPSec Settings）] ステップでの選択に応じて、対応する IKEv プロポーザルを使用できます。

IPSec 設定の詳細については、「IPSec プロポーザルの設定」を参照してください。

1. [IKEv2 IPSecプロポーザルの追加（Add IKEv2 IPSec Proposals）] をクリックし、ピア 1 とピア 2 に使用する IKEv2 プロポーザルを選択します。
2. [Perfect Forward Secrecy対応のDiffie-Hellmanグループ（Diffie-Hellman Group for Perfect Forward Secrecy）] を選択します。詳細については、「VPN で使用される暗号化アルゴリズムとハッシュアルゴリズム （13 ページ）」を参照してください。
3. [Next] をクリックします。

ステップ 11 [終了（Finish）] エリアに、完了した構成の概要が表示されます。

設定を確認し、問題がなければ [送信（Submit）] をクリックします。

ステップ 12

ステップ 13 次の手順を実行して、Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense デバイスに設定を展開します。

a) **Administration** > **Integrations** > **Firewall Management Center** を選択します。
b) **クラウド提供型 FMC** に対応するチェックボックスがオンになっていることを確認し、右側の [アクション（Actions）] ペインで [展開（Deployment）] をクリックします。
c) サイト間 VPN 設定に関係しているデバイスを選択し、[展開（Deploy）] をクリックします。
d) [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。Security Cloud Control で設定したのと同じ VPN トポロジが表示されます。

Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense と Multicloud Defense 間のサイト間 VPN トンネルの作成

（注） 新規のお客様が Security Cloud Control を使用して、Multicloud Defense と Cloud-Delivered Firewall Management Centerで管理される Firewall Threat Defense デバイス間のサイト間 VPN を設定する場合は、Cisco Technical Assistance Center（Cisco TAC）に連絡してこの機能を有効にしてください。ASA と Multicloud Defense 間のサイト間 VPN を手動で設定するには、Multicloud Defense アプリケーションで VPN を設定し、Cloud-Delivered Firewall Management Center で管理する Firewall Threat Defense デバイスにも手動で設定して、サイト間 VPN を起動します。

Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense と Multicloud Defense の間に、関連するすべての標準に準拠する Security Cloud Control ダッシュボードからサイト間 IPSec 接続を作成できます。VPN 接続が確立されると、ファイアウォールの背後にあるホストは、セキュアな VPN トンネルを介してゲートウェイの背後にあるホストに接続できます。

Multicloud Defense は現在、Amazon Web Services（AWS）、Azure、Google Cloud Platform（GCP）、および Oracle OCI クラウドアカウントをサポートしています。

次の手順を使用して、Security Cloud Control ダッシュボードから Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense デバイスと Multicloud Defense 間に VPN トンネルを作成します。

始める前に

次の前提条件を満たしていることを確認してください。

- Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense デバイスには保留中の変更がない必要があります。
- Multicloud Defense を Security Cloud Control にオンボードする必要があります。「クラウドアカウントの接続」を参照してください。
- Multicloud Defense Gateway は [アクティブ（Active）] 状態である必要があります。
- Multicloud Defense Gateway で VPN が有効になっている必要があります。「ゲートウェイ内で VPN を有効にする」を参照してください。
- 詳細については、「Multicloud Defense Gateway 前提条件と制限事項」を参照してください。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 ナビゲーションウィンドウで **Secure Connections** > **Network Connections** > **Site to Site VPN** を選択します。

ステップ 3 [トンネルの作成（Create Tunnel）]（  ）アイコンをクリックし、[サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 4 [ピアの選択（Peer Selection）] エリアで、次の情報を入力します。

- [設定名（Configuration Name）]：一意のトポロジ名を入力します。
- **ピア 1（Peer 1）**：**[FTD]** タブをクリックして、Firewall Threat Defense デバイスを選択します。
- **ピア 2（Peer 2）**： Multicloud Defense タブをクリックして、必要なゲートウェイを選択します。

  エクストラネットデバイスを選択する場合は、[静的（Static）] を選択して IP アドレスを指定し、DHCP が割り当てられた IP を持つエクストラネットデバイスの場合は [動的（Dynamic）] を選択します。[IPアドレス（IP Address）] には、静的インターフェイスの IP アドレスまたは動的インターフェイスの [DHCP割り当て（DHCP Assigned）] が表示されます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ピアの詳細（Peer Details）] エリアで、次の情報を入力します。

- **VPN アクセスインターフェイス（VPN Access Interface）**： Firewall Threat Defense のインターフェイスを選択してゲートウェイとの接続を確立します。
- [パブリックIP（Public IP）]（任意）：選択した Firewall Threat Defense の外部インターフェイスにマッピングする NAT のパブリック IP アドレスを指定します。
- ルーティング（Routing）：[Add Networks] をクリックし、Firewall Threat Defense から 1 つ以上の保護されたネットワークを選択して、選択したネットワークと Multicloud Defense Gateway の間にサイト間トンネルを作成します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [トンネルの詳細（Tunnel Details）] エリアで、次の情報を入力します。

- **仮想トンネルインターフェイス IP**：ピアの新しい **仮想トンネルインターフェイス** のアドレスを指定します。このデバイスで現在使用されていない未使用の IP アドレスを割り当てられます。
- [自律システム番号（Autonomous System Number）]：ネットワークの自律システム番号を指定します。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [IKE設定（IKE Settings）] エリアで、[IKEv2の追加（Add IKEv2）] をクリックし、インターネット キー エクスチェンジ（IKE）ネゴシエーションの IKE バージョンを追加して、プライバシー設定を指定します。

Security Cloud Control デフォルトの **[Local Pre-Shared Key]** が生成されます。このキーは、ピアで設定される秘密鍵文字列です。IKE では、認証フェーズでこのキーが使用されます。このキーは、ピア間にトンネルを確立する際の相互検証に使用されます。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 **[IPSec Settings]** エリアで **[Add IKEv2 IPSec Proposals]** をクリックして、IKE IPSec 設定を選択します。使用できるプロポーザルは、[IKE設定（IKE Settings）] ステップでの選択内容によって異なります。「IPSec プロポーザルの設定」を参照してください。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 [終了（Finish）] エリアで設定を確認し、設定に問題がない場合にのみ続行します。

ステップ 15 **[送信（Submit）]** をクリックします。

設定が Multicloud Defense Gateway にプッシュされます。

ステップ 16 次の手順を実行して、Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense デバイスに設定を展開します。

a) **Administration** > **Integrations** > **Firewall Management Center** を選択します。
b) **クラウド提供型 FMC** に対応するチェックボックスがオンになっていることを確認し、右側の [アクション（Actions）] ペインで [展開（Deployment）] をクリックします。
c) サイト間 VPN 設定に関係しているデバイスを選択し、[展開（Deploy）] をクリックします。
d) [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。Security Cloud Control で設定したのと同じ VPN トポロジが表示されます。

Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense と Secure Firewall ASA 間のサイト間 VPN の作成

始める前に

Firewall Threat Defense デバイスに保留中の展開があってはなりません。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 ナビゲーションウィンドウで **Secure Connections** > **Network Connections** > **Site to Site VPN** を選択します。

ステップ 3 [トンネルの作成（Create Tunnel）]（  ）アイコンをクリックし、[サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 4 [ピアの選択（Peer Selection）] エリアで、次の情報を入力します。

- [設定名（Configuration Name）]：一意のトポロジ名を入力します。

トポロジには、Firewall Threat Defense デバイス VPN であることとトポロジタイプを示す名前を付けることをお勧めします。

- **ピア 1（Peer 1）**：**[FTD]** タブをクリックして、Firewall Threat Defense デバイスを選択します。
- [ピア2（Peer 2）]：[ASA] タブをクリックして、Secure Firewall ASA デバイスを選択します。

  エクストラネットデバイスを選択する場合は、[静的（Static）] を選択して IP アドレスを指定し、DHCP が割り当てられた IP を持つエクストラネットデバイスの場合は [動的（Dynamic）] を選択します。[IPアドレス（IP Address）] には、静的インターフェイスの IP アドレスまたは動的インターフェイスの [DHCP割り当て（DHCP Assigned）] が表示されます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ピアの詳細（Peer Details）] エリアで、次の情報を入力します。

- [VPNアクセスインターフェイス（VPN Access Interface）]：ピア 1 とピア 2 の両方のインターフェイスを選択して、それらの間に接続を確立します。
- **LAN インターフェイス（LAN Interfaces）**：LAN サブネットを制御するピア 1 とピア 2 の両方のインターフェイスを選択します。複数のインターフェイスを選択できます
- [ルーティング（Routing）]：[ネットワークの追加（Add Networks）] をクリックし、ピア 1 とピア 2 に対して 1 つ以上の保護されたネットワークを選択して、それらの間にサイト間トンネルを作成します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [トンネルの詳細（Tunnel Details）] エリアで、次の情報を入力します。

- **仮想トンネルインターフェイスIP（Virtual Tunnel Interface IP）**：Secure Firewall ASA の新しい **[Virtual Tunnel Interfaces]** のアドレスを指定します。Security Cloud Control から Secure Firewall ASA のサンプルアドレスが提供されますが、競合が発生した場合は変更できます。このデバイスで現在使用されていない未使用の IP アドレスを割り当てられます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [IKE設定（IKE Settings）] エリアで、インターネット キー エクスチェンジ（IKE）のネゴシエーション中に使用する IKE バージョンを選択し、プライバシー設定を指定します。IKE ポリシーの詳細については、「グローバル IKE ポリシーの設定」を参照してください。

（注）
IKE ポリシーはデバイスに対してグローバルであり、デバイスに関連付けられたすべての VPN トンネルに適用されます。したがって、ポリシーを追加または削除すると、このデバイスが参加しているすべての VPN トンネルに影響します。

1. 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。

   （注）

デフォルトでは、[IKEVバージョン2] が有効になっています。

2. [IKEv2ポリシーの追加（Add IKEv2 Policies）] をクリックし、ピア 1 とピア 2 の IKEv2 ポリシーを選択します。
3. 参加デバイスの [ローカル事前共有キー（Local Pre-Shared Key）] と [リモート事前共有キー（Remote Pre-Shared Key）] が自動生成されます。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。
4. [IKEバージョン1（IKE Version 1）] をクリックして有効にします。
5. [IKEv1ポリシーの追加（Add IKEv1 Policies）] をクリックし、ピア 1 とピア 2 の IKEv1 ポリシーを選択します。
6. [IPEv1事前共有キー（IPEv1 Pre-Shared Key）] が自動生成されます。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [IPSec設定（IPSec Settings）] エリアで、ピア 1 およびピア 2 の IPSec 設定を指定します。[IPSec 設定（IPSec Settings）] ステップでの選択に応じて、対応する IKEv プロポーザルを使用できます。

IPSec 設定の詳細については、「IPSec プロポーザルの設定」を参照してください。

1. [IKEv2 IPSecプロポーザルの追加（Add IKEv2 IPSec Proposals）] をクリックし、ピア 1 とピア 2 に使用する IKEv2 プロポーザルを選択します。
2. [Perfect Forward Secrecy対応のDiffie-Hellmanグループ（Diffie-Hellman Group for Perfect Forward Secrecy）] を選択します。詳細については、「使用する Diffie-Hellman 係数グループの決定」を参照してください。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 [終了（Finish）] エリアに、完了した構成の概要が表示されます。

設定を確認し、問題がなければ [送信（Submit）] をクリックします。

ステップ 15 次の手順を実行して、Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense デバイスに設定を展開します。

a) **Administration** > **Integrations** > **Firewall Management Center** を選択します。
b) **クラウド提供型 FMC** に対応するチェックボックスがオンになっていることを確認し、右側の [アクション（Actions）] ペインで [展開（Deployment）] をクリックします。
c) サイト間 VPN 設定に関係しているデバイスを選択し、[展開（Deploy）] をクリックします。
d) [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。Security Cloud Control で設定したのと同じ VPN トポロジが表示されます。

サイト間 VPN の Secure Firewall ASA

Security Cloud Control は、Secure Firewall ASA デバイスの備えるサイト間 VPN 機能の次の側面をサポートしています。

- IPsec IKEv1 および IKEv2 プロトコルの両方をサポート。
- 自動または手動の事前共有認証キー。
- IPv4 および IPv6 内部、外部のすべての組み合わせをサポート。
- IPsec IKEv2 サイト間 VPN トポロジにより、セキュリティ認定に準拠するための設定を提供。
- スタティック インターフェイスおよびダイナミック インターフェイス。
- エクストラネットデバイスのスタティックまたはダイナミック IP アドレスをエンドポイントとしてサポート。

動的にアドレス指定されたピアによるサイト間 VPN 接続の設定

Security Cloud Control を使用すると、ピアのいずれかの VPN インターフェイス IP アドレスが不明な場合、またはインターフェイスが DHCP サーバーからアドレスを取得する場合に、ピア間にサイト間 VPN 接続を作成できます。事前共有キー、IKE 設定、および IPsec 設定が別のピアと一致するダイナミックピアは、サイト間 VPN 接続を確立できます。

A と B の 2 つのピアがあるとします。スタティックピアは、VPN インターフェイスの IP アドレスが固定されているデバイスであり、ダイナミックピアは、VPN インターフェイスの IP アドレスが不明であるか、一時的な IP アドレスを持つデバイスです。

次の使用例では、動的にアドレス指定されたピアとの安全なサイト間 VPN 接続を確立するためのさまざまなシナリオについて説明します。

- A はスタティックピア、B はダイナミックピア、またはその逆です。
- A はスタティックピア、B は DHCP サーバーから解決された IP アドレスを持つダイナミックピア、またはその逆です。
- A はダイナミックピアで、B はスタティックまたはダイナミック IP アドレスを持つエクストラネットデバイスです。
- A は DHCP サーバーからの解決済み IP アドレスを持つダイナミックピアで、B はスタティックまたはダイナミック IP アドレスを持つエクストラネットデバイスです。

（注） Adaptive Security Device Manager（ASDM）などのローカルマネージャを使用してインターフェイスの IP アドレスを変更すると、Security Cloud Control では、そのピアの [設定ステータス（Configuration Status）] に [競合検出（Conflict Detected）] と表示されます。このアウトオブバンドの変更を解決すると、他方のピアの [設定ステータス（Configuration Status）] が [未同期（Not Synced）] 状態に変わります。[未同期（Not Synced）] 状態のデバイスに Security Cloud Control 設定を展開する必要があります。

通常、ダイナミックピアの IP アドレスを他方のピアは把握していないため、ダイナミックピアから接続を開始する必要があります。リモートピアが接続を確立しようとすると、他方のピアは事前共有キー、IKE 設定、および IPsec 設定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。

（注） 次のシナリオでは、サイト間 VPN 接続を設定できません。

1 台のデバイスに複数のダイナミックピア接続がある場合。

- 3 台のデバイス A、B、C があるとします。
- A（スタティックピア）と B（ダイナミックピア）間のサイト間 VPN 接続を設定します。
- エクストラネットデバイスを作成して、A と C（ダイナミックピア）間のサイト間 VPN 接続を設定します。A のスタティック VPN インターフェイス IP アドレスをエクストラネットデバイスに割り当て、C との接続を確立します。

Secure Firewall ASA サイト間 VPN のガイドラインと制約事項

- Security Cloud Control は、S2S VPN の対象トラフィックを設計するための crypto-acl をサポートしていません。保護されたネットワークのみをサポートします。
- IKE ポート 500/4500 が使用されている場合、またはアクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、サイト間 VPN を同じポートに設定することはできません。
- トンネルモードにのみ対応し、トランスポートモードには対応していません。IPsec トンネル モードは、新しい IP パケットのペイロードになる元の IP データグラム全体を暗号化します。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。

- このリリースでは、1 つ以上の VPN トンネルを含む PTP トポロジのみがサポートされています。ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。

仮想トンネル インターフェイスの注意事項

- VTI は IPsec モードのみで設定可能です。Secure Firewall ASA で GRE トンネルを終了することはサポートされていません。
- トンネルインターフェイスを使用するトラフィックには、動的または静的なルートを使用することができます。
- VTI の MTU は、基盤となる物理インターフェイスに応じて自動的に設定されます。ただし、VTI を有効にした後で物理インターフェイス MTU を変更した場合は、新しい MTU 設定を使用するために VTI を無効にしてから再度有効にする必要があります。
- ネットワーク アドレス変換を適用する必要がある場合、IKE および ESP パケットは、UDP ヘッダーにカプセル化されます。
- 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。
- トンネル グループ名は、ピアが自身の IKEv1 または IKEv2 識別情報として送信するものと一致する必要があります。
- LAN-to-LAN トンネル グループの IKEv1 では、トンネルの認証方式がデジタル証明書である場合、かつ/またはピアがアグレッシブ モードを使用するように設定されている場合、IP アドレス以外の名前を使用できます。
- 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、VTI 設定と暗号マップの設定を同じ物理インターフェイスに共存させることができます。
- デフォルトでは、VTI 経由のトラフィックは、すべて暗号化されます。
- VTI インターフェイスのデフォルトのセキュリティレベルは 0 です。
- VTI経由のトラフィックを制御するため、VTIインターフェイスにアクセス リストを適用することができます。
- VTI では BGP のみサポートされます。
- Secure Firewall ASA 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この L2L セッションのモード CFG 属性を Secure Firewall ASA が取得できないため、IOS での設定交換要求を無効にします。
- IPv6 はサポートされていません。

関連情報：

- Secure Firewall ASA 間のサイト間 VPN トンネルの作成　（43 ページ）

Secure Firewall ASA 間のサイト間 VPN トンネルの作成

次の手順を使用して、2 つの ASA またはエクストラネットデバイスを備えた ASA 間にサイト間 VPN トンネルを作成します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**[セキュアな接続（Secure Connections）]**>**[サイト間 VPN（Site to Site VPN）]**> **[ASA と FDM（ASA & FDM）]** をクリックします。

ステップ 3 [トンネルの作成（Create Tunnel）]（  ）アイコンをクリックし、[サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 4

ステップ 5 [ピアの選択（Peer Selection）] エリアで、次の情報を入力します。

- [設定名（Configuration Name）]：一意のトポロジ名を入力します。
- [ピア1（Peer 1）]：[ASA] タブをクリックして、Secure Firewall ASA デバイスを選択します。
- [ピア2（Peer 2）]：[ASA] タブをクリックして、Secure Firewall ASA デバイスを選択します。

  エクストラネットデバイスを選択する場合は、[静的（Static）] を選択して IP アドレスを指定し、DHCP が割り当てられた IP を持つエクストラネットデバイスの場合は [動的（Dynamic）] を選択します。[IPアドレス（IP Address）] には、静的インターフェイスの IP アドレスまたは動的インターフェイスの [DHCP割り当て（DHCP Assigned）] が表示されます。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [ピアの詳細（Peer Details）] エリアで、次の情報を入力します。

- いずれかのオプションを選択して、新しい**ポリシーベース**または**ルートベース**のサイト間 VPN を作成します。
- [VPNアクセスインターフェイス（VPN Access Interface）]：ピア 1 とピア 2 の両方のインターフェイスを選択して、それらの間に接続を確立します。
- （ルートベースに適用可能）[LANインターフェイス（LAN Interfaces）]：LAN サブネットを制御するピア 1 とピア 2 の両方のインターフェイスを選択します。複数のインターフェイスを選択できます
- [ルーティング（Routing）]：[ネットワークの追加（Add Networks）] をクリックし、ピア 1 とピア 2 に対して 1 つ以上の保護されたネットワークを選択して、それらの間にサイト間トンネルを作成します。

- （ポリシーベースに適用可能）[NAT免除（NAT Exempt）] を選択して、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 ポリシーから除外します。個々のピアに対して手動で設定する必要があります。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については、「NAT からの ASA サイト間 VPN トラフィックの除外」を参照してください。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 （ルートベースに適用可能）[トンネルの詳細（Tunnel Details）] では、前の手順でピア デバイスを設定すると、[VTIアドレス（VTI Address）] フィールドが自動的に入力されます。必要に応じて、新しい VTI として使用される IP アドレスを手動で入力できます。

ステップ 10 [IKE設定（IKE Settings）] エリアで、インターネット キー エクスチェンジ（IKE）ネゴシエーション中に使用する IKE バージョンを選択し、プライバシー設定を指定します。IKE ポリシーの詳細については、グローバル IKE ポリシーについてを参照してください。

（注）
IKE ポリシーはデバイスに対してグローバルであり、デバイスに関連付けられたすべての VPN トンネルに適用されます。したがって、ポリシーを追加または削除すると、このデバイスが参加しているすべての VPN トンネルに影響します。

1. 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。

   （注）
   デフォルトでは、[IKEVバージョン2] が有効になっています。

2. [IKEv2ポリシーの追加（Add IKEv2 Policies）] をクリックし、ピア 1 とピア 2 の IKEv2 ポリシーを選択します。
3. 参加デバイスの [ローカル事前共有キー（Local Pre-Shared Key）] と [リモート事前共有キー（Remote Pre-Shared Key）] が自動生成されます。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。
4. [IKEバージョン1（IKE Version 1）] をクリックして有効にします。
5. [IKEv1ポリシーの追加（Add IKEv1 Policies）] をクリックし、ピア 1 とピア 2 の IKEv1 ポリシーを選択します。
6. [IPEv1事前共有キー（IPEv1 Pre-Shared Key）] が自動生成されます。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [IPSec設定（IPSec Settings）] エリアで、ピア 1 およびピア 2 の IPSec 設定を指定します。[IPSec設定（IPSec Settings）] ステップでの選択に応じて、対応する IKEv プロポーザルを使用できます。

IPSec 設定の詳細については、「グローバル IKE ポリシーについて」を参照してください。

1. [IKEv2 IPSecプロポーザルの追加（Add IKEv2 IPSec Proposals）] をクリックし、ピア 1 とピア 2 に使用する IKEv2 プロポーザルを選択します。
2. [Perfect Forward Secrecy対応のDiffie-Hellmanグループ（Diffie-Hellman Group for Perfect Forward Secrecy）] を選択します。詳細については、「VPN で使用される暗号化アルゴリズムとハッシュアルゴリズム （13 ページ）」を参照してください。

ステップ 13 [終了（Finish）] エリアで設定を確認し、設定に問題がない場合にのみ続行します。

デフォルトでは、[変更をCisco ASAにすぐに展開する（Deploy changes to Cisco ASA）] チェックボックスがオンになっており、[送信（Submit）] をクリックすると設定がすぐに Cisco ASA デバイスに展開されます。

後で設定を確認して手動で展開する場合は、このチェックボックスをオフにします。

新しく構成されたサイト間 VPN トンネルを示す [VPNトンネル（VPN Tunnels）] ページに移動します。変更は段階的であり、手動で展開する必要があります。VTI トンネルを介してデバイス間でVTI トラフィックを自動的にルーティングするルーティングポリシーが作成されます。このポリシーを表示するには、[セキュリティデバイス（Security Devices）] ページでデバイスを選択し、[設定（Configuration）] > [差分（Diff）] の順に選択します。

Cisco ASA と Multicloud Defense Gateway 間でのサイト間 VPN の作成

（注） 新規のお客様が Security Cloud Control を使用して Multicloud Defense と Cisco ASA デバイス間のサイト間 VPN を設定する場合は、Cisco Technical Assistance Center （Cisco TAC）に連絡してこの機能を有効にしてください。

Cisco ASA と Multicloud Defense 間のサイト間 VPN を手動で構成するには、Multicloud Defense アプリケーションと Cisco ASA デバイスで VPN を手動で構成して、サイト間 VPN を起動します。

Cisco ASA と、関連するすべての標準に準拠する Multicloud Defense Gateway の間にサイト間 IPsec 接続を作成できます。VPN 接続が確立されると、ファイアウォールの背後にあるホストは、セキュアな VPN トンネルを介してゲートウェイの背後にあるホストに接続できます。

Multicloud Defense は現在、Amazon Web Services（AWS）、Azure、Google Cloud Platform（GCP）、および Oracle OCI クラウドアカウントをサポートしています。

次の手順を使用して、Security Cloud Control ダッシュボードから Security Cloud Control および Multicloud Defense Gateway によって管理される Cisco ASA デバイス間に VPNトンネルを作成します。

始める前に

次の前提条件を満たしていることを確認してください。

- Cisco ASA デバイスには保留中の変更がない必要があります。
- VPN トンネルを作成する前に、Cisco ASA コンソールで BGP プロファイルを作成します。詳細については、「Cisco ASA ボーダーゲートウェイプロトコルの設定」を参照してください。
- Multicloud Defense Gateway は [アクティブ（Active）] 状態である必要があります。
- Multicloud Defense Gateway で VPN が有効になっている必要があります。「ゲートウェイ内で VPN を有効にする」を参照してください。
- 詳細については、「Cisco ASA のサイト間 VPN の制限事項とガイドライン」を参照してください。
- 詳細については、「Multicloud Defense Gateway 前提条件と制限事項」を参照してください。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** を選択します。

ステップ 3 [トンネルの作成（Create Tunnel）]（  ）アイコンをクリックし、[サイト間VPN（Site-to-Site VPN）] をクリックします。

ステップ 4 [ピアの選択（Peer Selection）] エリアで、次の情報を入力します。

- [設定名（Configuration Name）]：一意のトポロジ名を入力します。
- [ピア1（Peer 1）]：[ASA] タブをクリックして、Secure Firewall ASA デバイスを選択します。
- **ピア 2（Peer 2）**：**[Multicloud Defense]** タブをクリックし、マルチクラウドゲートウェイを選択します。

  エクストラネットデバイスを選択する場合は、[静的（Static）] を選択して IP アドレスを指定し、DHCP が割り当てられた IP を持つエクストラネットデバイスの場合は [動的（Dynamic）] を選択します。[IPアドレス（IP Address）] には、静的インターフェイスの IP アドレスまたは動的インターフェイスの [DHCP割り当て（DHCP Assigned）] が表示されます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ピアの詳細（Peer Details）] エリアで、次の情報を入力します。

- **VPN アクセスインターフェイス（VPN Access Interface）**：Multicloud Defense Gateway への接続を確立するための Secure Firewall ASA インターフェイスを選択します。

- **LAN インターフェイス（LAN Interfaces）**：LAN サブネットを制御する Secure Firewall ASA のインターフェースを選択します。複数のインターフェイスを選択できます
- [パブリックIP（Public IP）]（任意）：選択した Secure Firewall ASA の外部インターフェイスにマッピングする NAT のパブリック IP アドレスを指定します。
- **ルーティング（Routing）**：**ネットワークの追加（Add Networks）** をクリックし、Secure Firewall ASA の 1 つ以上の保護されたネットワークを選択して、Multicloud Defense Gateway とのサイト間トンネルを確立します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [トンネルの詳細（Tunnel Details）] エリアで、次の情報を入力します。

- **仮想トンネルインターフェイス IP（Virtual Tunnel Interface IP）**：ピアの新しい **[Virtual Tunnel Interfaces]** のアドレスを指定します。Security Cloud Control から Secure Firewall ASA のサンプルアドレスが提供されますが、競合が発生した場合は変更できます。このデバイスで現在使用されていない未使用の IP アドレスを割り当てられます。
- **自律システム番号（Autonomous System Number）**（ピア 1）：Secure Firewall ASA デバイスに自律システム番号が設定されていない場合、Security Cloud Control からデバイスの自律システム番号が提示されますが、その番号は変更できます。デバイスに自律システム番号がすでに設定されている場合は、現在の値が表示され、変更できません。
- [自律システム番号（Autonomous System Number）]（ピア 2）：BGP プロファイルが Multicloud Defense Gateway に割り当てられている場合、プロファイルに関連付けられた自律番号が表示され、変更できません。「Multicloud Defense Gateway の追加」を参照してください。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 **[IKE Settings]** エリアで、Security Cloud Control によってデフォルトの **[Pre-Shared Key]** が生成されます。このキーは、ピアで設定される秘密鍵文字列です。IKE では、認証フェーズでこのキーが使用されます。このキーは、ピア間にトンネルを確立する際の相互検証に使用されます。

ステップ 11 [終了（Finish）] エリアで設定を確認し、設定に問題がない場合にのみ続行します。

デフォルトでは、[変更をCisco ASAにすぐに展開する（Deploy changes to Cisco ASA）] チェックボックスがオンになっており、[送信（Submit）] をクリックすると設定がすぐに Cisco ASA デバイスに展開されます。

後で設定を確認して手動で展開する場合は、このチェックボックスをオフにします。

ステップ 12 **[送信（Submit）]** をクリックします。

設定が Multicloud Defense Gateway にプッシュされます。

Security Cloud Control の [VPN] ページには、ピア間で作成されたサイト間トンネルが表示されます。対応するトンネルは Multicloud Defense Gateway ポータルで確認できます。

NAT からのサイト間 VPN トラフィックの除外

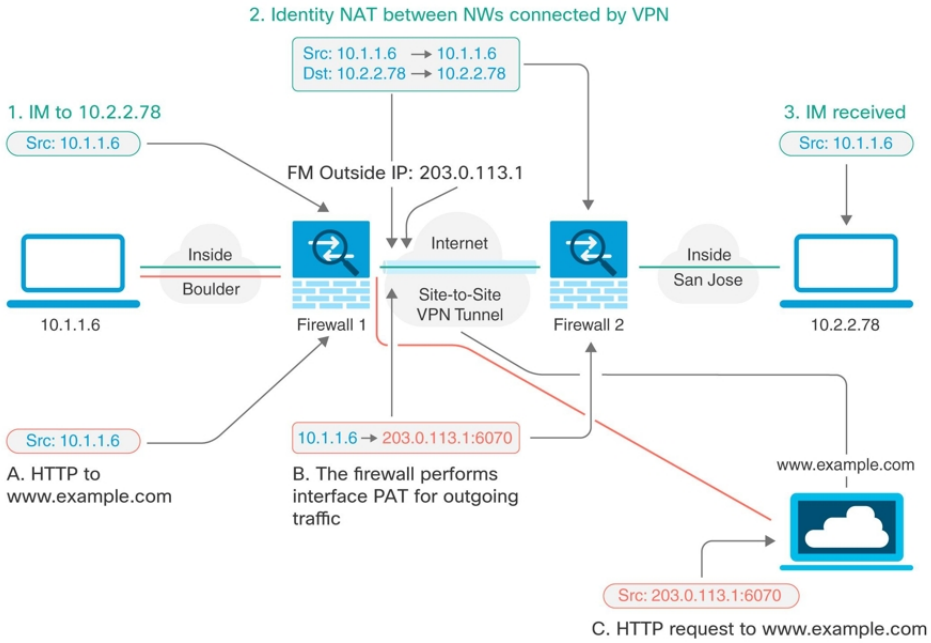
インターフェイスでサイト間 VPN 接続が定義されていて、かつそのインターフェイス向けの NAT ルールを指定している場合、NAT ルールから VPN 上のトラフィックを任意で除外できます。この操作は、VPN 接続のリモート エンドが内部アドレスを処理できる場合に行うと便利です。

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 ポート アドレス変換（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。



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。

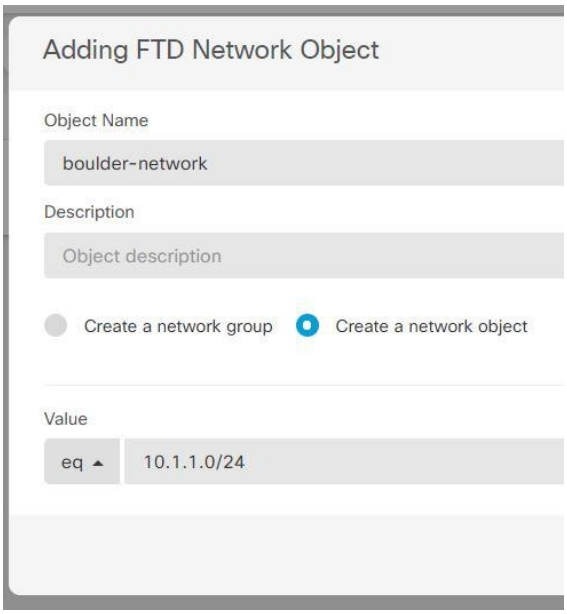
手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 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。

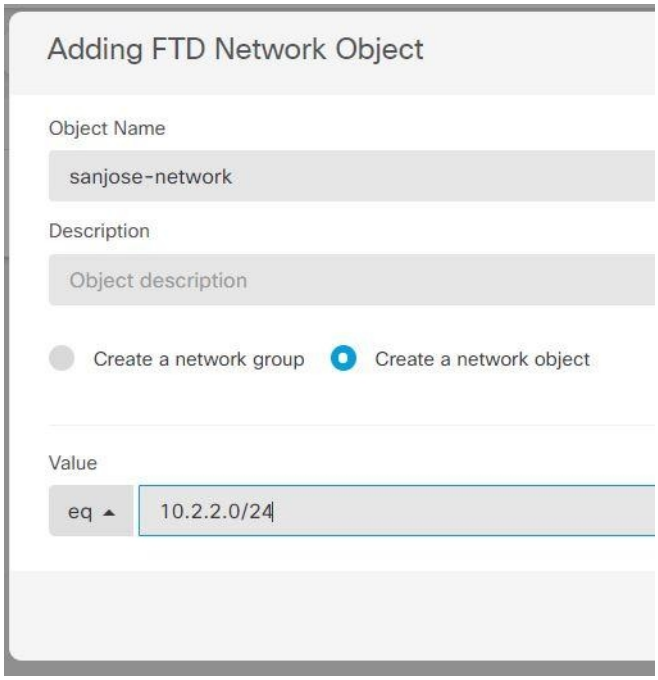
1. 左側のペインで [オブジェクト（Objects）] をクリックします。
2. 青色のプラスボタン をクリックして、オブジェクトを作成します。
3. **[FTD]** > **[ネットワーク（Network）]** をクリックします。
4. ネットワーク内でボールダーを特定します。
5. オブジェクト名を入力します（例：boulder-network）。

6. [ネットワークオブジェクトの作成（Create a network object）] を選択します。
7. [値（Value）] セクションで、次の手順を実行します。
   - [eq] を選択して、単一の IP アドレスまたは CIDR 表記で表されるサブネットアドレスを入力します。
   - [範囲（range）] を選択し、IP アドレスの範囲を入力します。たとえば、ネットワークアドレスを 10.1.1.0/24 と入力します。



8. [追加（Add）] をクリックします。
9. 青色のプラスボタン + をクリックして、オブジェクトを作成します。
10. サンノゼの内部ネットワークを定義します。
11. オブジェクト名を入力します（例：san-jose）。
12. [ネットワークオブジェクトの作成（Create a network object）] を選択します。
13. [値（Value）] セクションで、次の手順を実行します。
    - [eq] を選択して、単一の IP アドレスまたは CIDR 表記で表されるサブネットアドレスを入力します。

- [範囲（range）] を選択し、IP アドレスの範囲を入力します。たとえば、ネットワークアドレスを 10.1.1.0/24 と入力します。

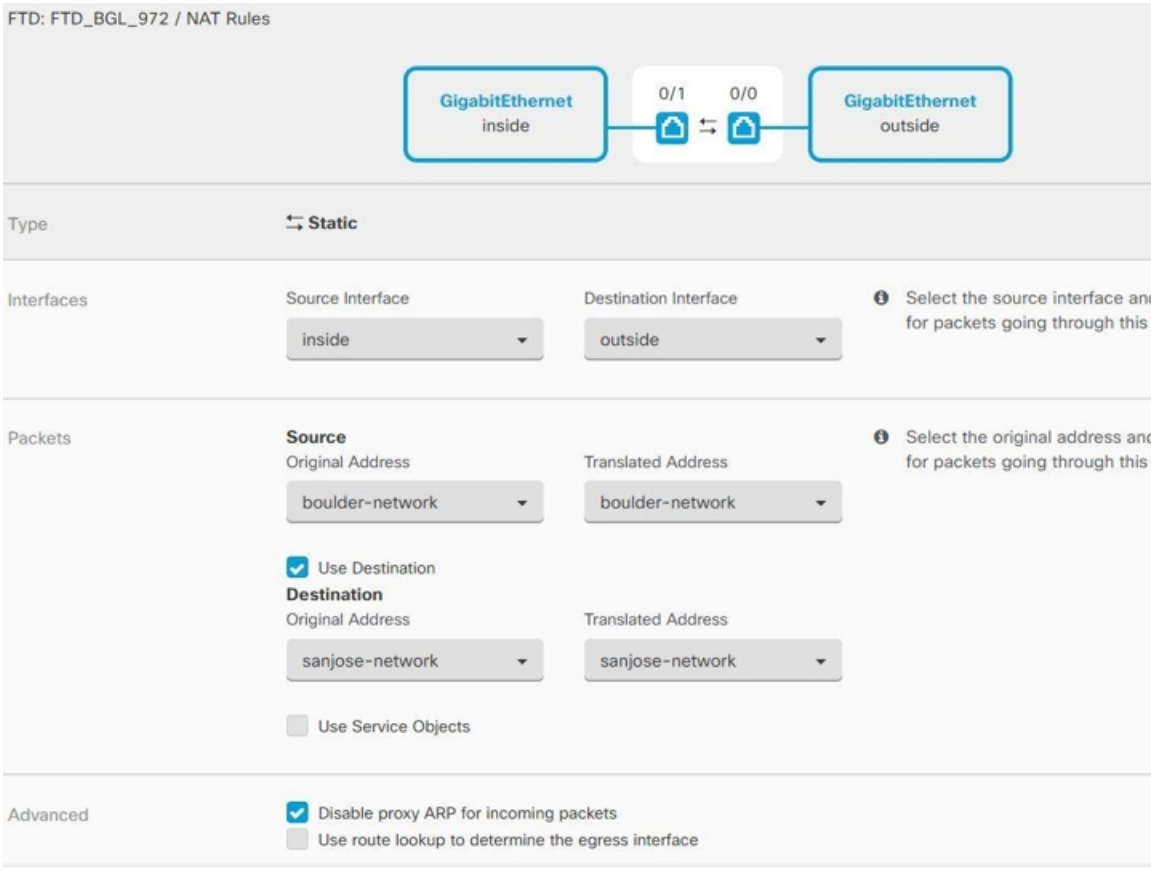


14. [追加（Add）] をクリックします。

ステップ 3 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。

1. 左側のペインで **[セキュリティデバイス（Security Devices）]** > **[すべてのデバイス（All Devices）]** の順にクリックします。
2. フィルタを使用して、NAT ルールを作成するデバイスを見つけます。
3. 詳細パネルの [管理（Management）] 領域で、[NAT] NAT をクリックします。
4. + > [Twice NAT] をクリックします。
   - セクション 1 で、[静的（Static）] を選択します。 [続行（Continue）] をクリックします。
   - セクション 2 で、[送信元インターフェイス（Source Interface）] = [内部（inside）] および [宛先インターフェイス（Destination Interface）] = [外部（outside）] を選択します。[続行（Continue）] をクリックします。
   - セクション 3 で、[送信元の元のアドレス（Source Original Address）] = 'boulder-network' および [送信元の変換後アドレス（Source Translated Address）] = 'boulder-network' を選択します。
   - [宛先を使用（Use Destination）] を選択します。

- [宛先の元のアドレス（Destination Original Address）] = 'sanjose-network' および [送信元の変換後アドレス（Source Translated Address）] = 'sanjose-network' を選択します。**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。

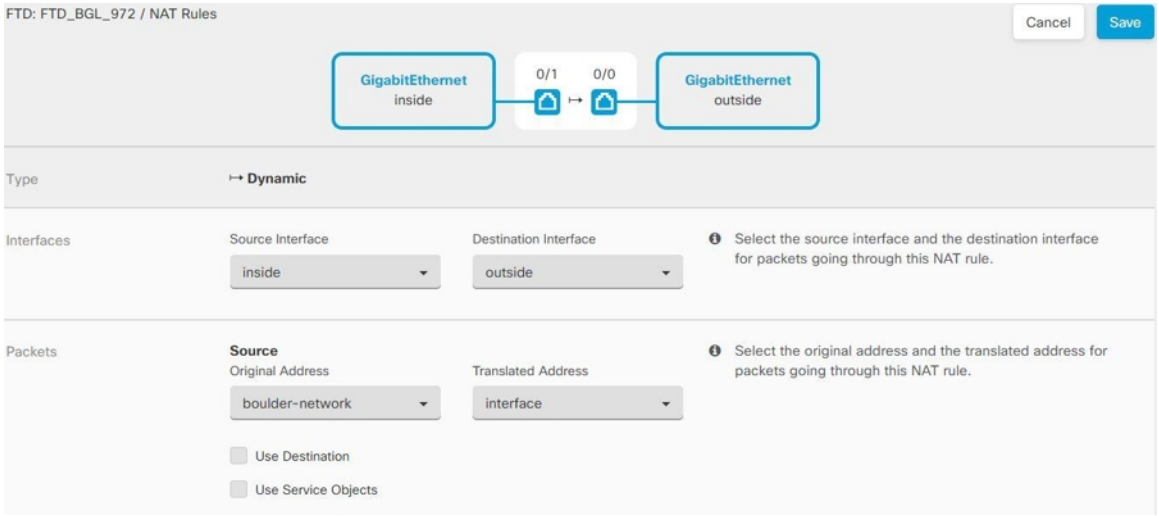


- [着信パケットのプロキシ ARP の無効化（Disable proxy ARP for incoming packets）] を選択します。
- [保存（Save）] をクリックします。
- 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 4 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：IPv4 トラフィックを対象とする内部インターフェイス用ダイナミック インターフェイス PAT ルールは、初期設定時にデフォルトで作成されるので、既に存在する可能性があります。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。

1.  > [Twice NAT] をクリックします。
2. セクション 1 で、[ダイナミック（Dynamic）] を選択します。[続行（Continue）] をクリックします。
3. セクション 2 で、[送信元インターフェイス（Source Interface）] = [内部（inside）] および [宛先インターフェイス（Destination Interface）] = [外部（outside）] を選択します。[続行（Continue）] をクリックします。
4. セクション 3 で、[送信元の元のアドレス（Source Original Address）] = 'boulder-network' および [送信元の変換後アドレス（Source Translated Address）]='インターフェイス（interface）' を選択します。



5. [保存（Save）] をクリックします。
6. 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 5 設定変更を Security Cloud Control に展開します。詳細については、「Security Cloud Control から FTD への設定変更の展開」を参照してください。

ステップ 6 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。

サイト間仮想プライベートネットワークのモニタリング

Security Cloud Control を使用すると、オンボード FDM-managed デバイスで既存または新たに作成されたサイト間 VPN 設定を監視、変更、および削除できます。

サイト間 VPN トンネルの接続の確認

[接続の確認（Check Connectivity）] ボタンを使用して、トンネルに対するリアルタイムの接続確認をトリガーし、トンネルの現在の状態（アクティブまたはアイドル）を確認します。サイト間 VPN トンネルを検索してフィルタ処理する （58 ページ）[オンデマンド接続確認（on-demand connectivity check）] ボタンをクリックしていない場合、オンボーディングされているすべてのデバイスで利用可能なすべてトンネルに対する確認が 1 時間に一度実行されます。

（注）
- Security Cloud Control は、トンネルがアクティブかアイドルかを判断するために、FTD で次の接続確認コマンドを実行します。

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- ASA モデルデバイストンネルは常に [アイドル（Idle）] と表示されます。

[VPN] ページからトンネル接続を確認するには、次の手順を実行します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** の順に選択します。

ステップ 3 サイト間 VPN トンネルのトンネルのリストを検索およびフィルタリングして、選択します。

ステップ 4 右側の [アクション（Actions）] ペインで、[接続の確認（Check Connectivity）] をクリックします。

[サイト間VPN（Site-to-Site VPN）] ダッシュボード

Security Cloud Control では、テナントで作成されたサイト間 VPN 接続に関する統合情報が表示されます。

1. Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。
2. 左側のペインで、[セキュアな接続（Secure Connections）] > [サイト間VPN（Site to Site VPN）] の順にクリックします。[サイト間VPN（Site-to-Site VPN）] には、次のウィジェットの情報が表示されます。

- [セッションとインサイト（Sessions and Insights）]：アクティブな VPN トンネルとアイドル状態の VPN トンネルをそれぞれ適切な色で表す棒グラフが表示されます。
- [問題（Issues）]：問題が検出されたトンネルの合計数が表示されます。
- [保留中の展開（Pending Deploy）]：展開が保留中のトンネルの合計数が表示されます。

円グラフの値またはウィジェット内のリンクをクリックすると、選択した値に基づき、フィルタを含むサイト間 VPN のリストページが表示されます。たとえば、[VPNトンネルステータス（VPN Tunnel Status）] ウィジェットで [アクティブなVPNトンネル（Active VPN Tunnels）] をクリックすると、[アクティブ（Active）] ステータスフィルタが適用されたサイト間 VPN のリストページが表示され、アクティブトンネルのみが表示されます。

VPN の問題の特定

Security Cloud Control は、FTD の VPN の問題を特定できます（この機能は、AWS VPC サイト間 VPN トンネルではまだ利用できません）。この記事では次のことを説明します。

- ピアが欠落している VPN トンネルを見つける
- 暗号化キーの問題がある VPN ピアを見つける
- トンネルに対して定義された不完全な、または誤った構成のアクセスリストを見つける
- トンネル構成の問題を見つける

トンネル設定の問題の解決 （57 ページ）

ピアが欠落している VPN トンネルを見つける

「Missing IP Peer」状態は、FDM-managed デバイスよりも Cisco ASA デバイスで発生する可能性が高くなります。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 [テーブルビュー（Table View）] を選択します。

ステップ 4 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 5 検出された問題を確認します。

ステップ 6 問題を報告している各デバイス⚠を選択し、右側の [ピア（Peers）] ペインを確認します。1 つのピア名がリストされます。Security Cloud Control は、他のピア名を「Missing peer IP」として報告します。

暗号化キーの問題がある VPN ピアを見つける

このアプローチを使用して、以下のような暗号化キーの問題がある VPN ピアを見つけます。

- IKEv1 または IKEv2 キーが無効、欠落しているか、一致しない
- トンネルが古くなっているか、暗号化レベルが低い

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 [テーブルビュー（Table View）] を選択します。

ステップ 4 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 5 問題を報告している各デバイス⚠を選択し、右側の [ピア（Peers）] ペインを確認します。ピア情報には、両方のピアが表示されます。

ステップ 6 いずれかのデバイスの [ピアの表示（View Peers）] をクリックします。

ステップ 7 ダイアグラムビューで、問題を報告しているデバイスをダブルクリックします。

ステップ 8 下部の [トンネルの詳細（Tunnel Details）] パネルで [Key Exchange（キー交換）] をクリックします。両方のデバイスを表示して、そこでキーの問題を診断できます。

トンネルに対して定義された不完全な、または誤った設定のアクセスリストを見つける

「アクセスリストが不完全または正しく設定されていない」状態は、ASA デバイスでのみ発生する可能性があります。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 [テーブルビュー（Table View）] を選択します。

ステップ 4 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 5 問題を報告している各デバイス⚠を選択し、右側の [ピア（Peers）] ペインを確認します。ピア情報には、両方のピアが表示されています。

ステップ 6 いずれかのデバイスの [ピアの表示（View Peers）] をクリックします。

ステップ 7 ダイアグラムビューで、問題を報告しているデバイスをダブルクリックします。

ステップ 8 下部の [トンネルの詳細（Tunnel Details）] パネルで [トンネルの詳細（Tunnel Details）] をクリックします。「ネットワーク ポリシー：不完全（Network Policy: Incomplete）」というメッセージが表示されます。

トンネル設定の問題を見つける

トンネル設定のエラーは、次のシナリオで発生する可能性があります。

- サイト間 VPN インターフェイスの IP アドレスが変更されたときの、「ピア IP アドレス値が変更されました（Peer IP Address Value has changed）」。
- VPN トンネルの IKE 値が他の VPN トンネルと一致しない場合、「IKE 値が一致しません（IKE value Mismatch）」というメッセージが表示されます。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 [テーブルビュー（Table View）] を選択します。

ステップ 4 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 5 [トンネルの問題（Tunnel Issues）] で、[検出された問題（Detected Issues）] をクリックして、エラーを報告している VPN 設定を表示します。問題を報告している（⚠）設定を表示できます。

ステップ 6 問題を報告している VPN 設定を選択します。

ステップ 7 右側の [ピア（Peers）] ペインに、問題のあるピアに ⚠ アイコンが表示されます。⚠ アイコンにカーソルを合わせると、問題と解決策が表示されます。

次のステップ：トンネル設定の問題の解決。

トンネル設定の問題の解決

この手順では、次のトンネル設定の問題を解決を試みます。

- サイト間 VPN インターフェイスの IP アドレスが変更されたときの、「ピア IP アドレス値が変更されました（Peer IP Address Value has changed）」。
- VPN トンネルの IKE 値が他の VPN トンネルと一致しない場合、「IKE 値が一致しません（IKE value Mismatch）」というメッセージが表示されます。

詳細については、「トンネル設定の問題を見つける」を参照してください。

手順

ステップ 1 左側のペインで [インベントリ（Inventory）]**Security Devices** をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、問題を報告している VPN 設定に関連付けられているデバイスを選択します。

ステップ 4 デバイスの変更を受け入れます。

ステップ 5 左側のペインで、**[VPN]** > **[ASA/FDMサイト間VPN（ASA/FDM Site-to-Site VPN）]** をクリックして VPN ページを開きます。

ステップ 6 この問題を報告している VPN 設定を選択します。

ステップ 7 [アクション（Actions）] ペインで、[編集（Edit）] アイコンをクリックします。

ステップ 8 各手順で [次へ（Next）] をクリックして、最後に手順 4 で [完了（Fnish）] ボタンをクリックします。

ステップ 9 すべてのデバイスの設定変更のプレビューと展開。

サイト間 VPN トンネルを検索してフィルタ処理する

フィルタサイドバー を検索フィールドと組み合わせて使用して、VPN トンネル図に示されている VPN トンネルの検索を絞り込みます。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 フィルタアイコン をクリックしてフィルタペインを開きます。

ステップ 4 これらのフィルタを使用して検索を絞り込みます。

- [デバイスによるフィルタ（Filter by Device）] - [デバイスによるフィルタ（Filter by Device）] をクリックし、[デバイスタイプ（Device Type）] タブを選択し、フィルタ処理で検索するデバイスをチェックします。
- [トンネルの問題（Tunnel Issues）] - トンネルの各サイドで問題が検出されたかどうかでフィルタ処理します。問題のあるデバイスの例には、関連するインターフェイス、ピア IP アドレス、アクセスリストが欠落している、IKEv1 プロポーザルが一致しないなどがありますが、これらに限定されません（トンネルの問題の検出は、AWS VPC VPN トンネルではまだ使用できません）。

- [デバイス/サービス（Devices/Services）] - デバイスのタイプでフィルタ処理します。
- [ステータス（Status）]– トンネルのステータスには、アクティブとアイドルがあります。
  - [アクティブ（Active）] - セッションが開かれ、ネットワークパケットが VPN トンネルを通過している、または正常なセッションが確立され、タイムアウトになっていない場合。アクティブのステータスは、トンネルが有効で関連していることを示します。
  - [アイドル（Idle）] - Security Cloud Control はこのトンネルのオープンセッションを検出できません。トンネルが使用されていないか、このトンネルに問題がある可能性があります。
- [オンボーディング済み（Onboarded）] - デバイスは、Security Cloud Control によって管理される場合と、Security Cloud Control によって管理されない場合（管理対象外）があります。
  - [管理対象（Managed）] - Security Cloud Control が管理するデバイスでフィルタ処理します。
  - [管理対象外（Unmanaged）] - Security Cloud Control が管理しないデバイスでフィルタ処理します。
- [デバイスタイプ（Device Types）] - トンネルの各サイドがライブデバイス（接続されたデバイス）かモデルデバイスかでフィルタ処理します。

ステップ 5 検索バーにデバイス名または IP アドレスを入力して、フィルタ処理された結果を検索することもできます。検索では大文字と小文字は区別されません。

管理対象外サイト間 VPN ピアのオンボーディング

ピアの 1 つがオンボードされると、Security Cloud Control がサイト間 VPN トンネルを検出します。2 番目のピアが Security Cloud Control の管理対象外の場合は、VPN トンネルのリストをフィルタ処理して、管理対象外デバイスを見つけてオンボードできます。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 [テーブルビュー（Table View）] を選択します。

ステップ 4 をクリックしてフィルタパネルを開きます。

ステップ 5 [管理対象外（Unmanaged）] にチェックを入れます。

ステップ 6 結果の表からトンネルを選択します。

ステップ 7 右側の [ピア（Peers）] ペインで、[デバイスのオンボード（Onboard Device）] をクリックし、画面の指示に従います。

サイト間 VPN トンネルの IKE オブジェクトの詳細の表示

選択したトンネルのピア/デバイスで設定されている IKE オブジェクトの詳細を表示できます。それらの詳細は、IKE ポリシーオブジェクトの優先順位に基づいた階層のツリー構造に表示されます。

（注） エクストラネットデバイスには、IKE オブジェクトの詳細が表示されません。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 [VPN トンネル（VPN Tunnels）] ページで、ピアを接続する VPN トンネルの名前をクリックします。

ステップ 4 右側の [関係（Relationships）] で、詳細を表示するオブジェクトを展開します。

サイト間 VPN トンネルが最後に正常に確立された日を表示する

この情報は通常、VPN トンネルが最後に正常に確立された日付と時刻を提供し、2 つのサイト間の接続を保証します。このデータにアクセスすることは、VPN の正常性をモニターしたり、発生する可能性のある接続の問題をトラブルシュートしたりすることができます。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 **[VPN Tunnels]** ページには、管理対象デバイス全体に設定されたすべてのサイト間 VPN トンネルが表示されます。トンネルをクリックすると、右側のペインで詳細を表示できます。

（注）
[Search and Filter Site-to-Site VPN Tunnels] を使用して、特定のトンネルを検索します。

[Last Active] フィールドには、VPN トンネルが正常に確立された日付と時刻が表示されます。

サイト間 VPN トンネル情報の表示

サイト間 VPN テーブルビューは、Security Cloud Control にオンボードされたすべてのデバイスで使用可能なすべてのサイト間 VPN トンネルの完全なリストです。トンネルは、このリストに 1 つだけ存在します。表にリストされているトンネルをクリックすると、右側のサイドバーにオプションが表示され、トンネルのピアに直接移動して詳細に調査できます。

Security Cloud Control がトンネルの両側を管理していない場合は、[オンボードデバイス（Onboard Device）] をクリックして、管理対象外のピアをオンボードするメインの [オンボード（Onboarding）] ページを開くことができます。管理対象外サイト間 VPN ピアのオンボーディング （59 ページ） Security Cloud Control がトンネルの両側を管理する場合、[ピア2（Peer 2）] 列には管理対象デバイスの名前が含まれています。ただし、AWS VPC の場合、[ピア2（Peer 2）] 列には VPN ゲートウェイの IP アドレスが含まれています。

テーブルビューでサイト間 VPN 接続を表示するには、次の手順を実行します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

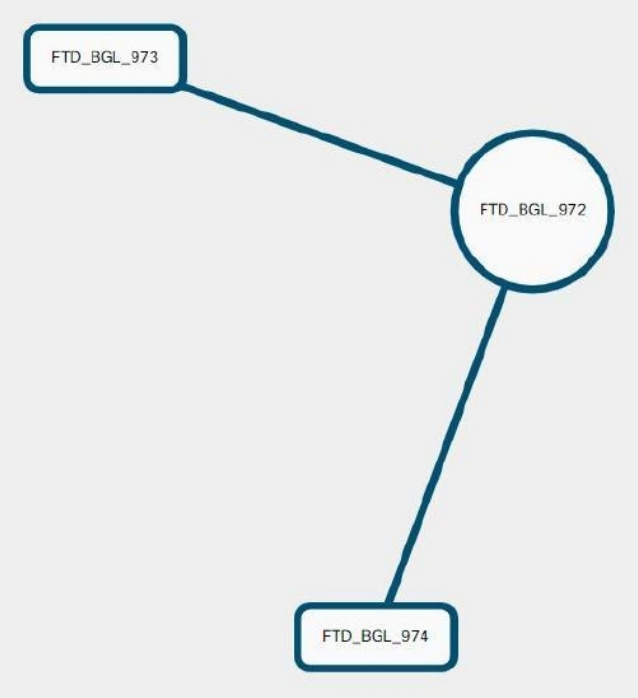
ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして VPN ページを開きます。

ステップ 3 **[VPN Tunnels]** ページには、管理対象デバイス全体に設定されたすべてのサイト間 VPN トンネルが表示されます。トンネルをクリックすると、右側のペインに詳細が表示されます。

（注）
[Search and Filter Site-to-Site VPN Tunnels] を使用して、特定のトンネルを検索します。

サイト間 VPN のグローバル表示

これは、グローバルビューの例です。この図では、「FTD_BGL_972」に FTD_BGL_973 デバイスと FTD_BGL_974 デバイスのサイト間接続があります。



手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックします。

ステップ 3 [グローバルビュー（Global view）] ボタンをクリックします。

ステップ 4 「サイト間 VPN トンネルの検索とフィルタ処理」を使用して特定のトンネルを見つけるか、グローバルビューのグラフィックを拡大して、探している VPN ゲートウェイとそのピアを見つけます。

ステップ 5 グローバルビューに表示されているピアのいずれかを選択します。

ステップ 6 **[詳細の表示（View Details）]** をクリックします。

ステップ 7 VPN トンネルのもう一方の端をクリックすると、その接続のトンネルの詳細、NAT 情報、およびキー交換情報が Security Cloud Control に表示されます。

- [トンネルの詳細（Tunnel Details）]：トンネルの名前と接続情報が表示されます。[更新（Refresh）] アイコンをクリックすると、トンネルの接続情報が更新されます。
- [AWS接続固有のトンネルの詳細（Tunnel Details specific to AWS connections）]：AWS サイト間接続のトンネルの詳細は、他の接続の場合と若干異なります。AWS VPC から VPN

ゲートウェイへの接続ごとに、AWS は 2 つの VPN トンネルを作成します。これは、高可用性を実現するためです。

- トンネルの名前は、VPN ゲートウェイが接続されている VPC の名前を表します。トンネルの名前に含まれている IP アドレスは、VPN ゲートウェイが VPC として認識している IP アドレスです。
- Security Cloud Control の接続ステータスが [アクティブ（Active）] の場合、AWS トンネルの状態は [アップ（Up）] です。Security Cloud Control の接続ステータスが [非アクティブ（Inactive）] の場合、AWS トンネルの状態は [ダウン（Down）] です。

- [NAT情報（NAT Information）]：使用されている NAT ルールのタイプ、元のパケットの情報、および変換されたパケットの情報が表示され、そのトンネルの NAT ルールを確認できる NAT テーブルへのリンクが提供されます（AWS VPC サイト間 VPN ではまだ利用できません）。
- [キー交換（Key Exchange）]：トンネルで使用されている暗号キーと、キー交換の問題が表示されます（AWS VPC サイト間 VPN ではまだ利用できません）。

[サイト間VPNトンネル（Site-to-Site VPN Tunnels）] ペイン

[トンネル（Tunnels）] ペインには、特定の VPN ゲートウェイに関連付けられているすべてのトンネルのリストが表示されます。VPN ゲートウェイと AWS VPC のサイト間 VPN 接続の場合、[トンネル（Tunnels）] ペインには、VPN ゲートウェイから VPC へのすべてのトンネルが表示されます。VPN ゲートウェイと AWS VPC のサイト間 VPN 接続にはそれぞれ 2 つのトンネルがあるため、他のデバイスで通常表示される 2 倍の数のトンネルが表示されます。

VPN ゲートウェイの詳細

VPN ゲートウェイに接続されているピア数と、VPN ゲートウェイの IP アドレスが表示されます。これは、[VPNトンネル（VPN Tunnels）] ページにのみ表示されます。

ピアの表示

サイト間 VPN ピアのペアを選択すると、ペアリングされた 2 つのデバイスのリストが [ピア（Peers）] ペインに表示され、いずれかのデバイスの [ピアの表示（View Peer）] をクリックできます。[ピアの表示（View Peer] をクリックすると、そのデバイスが関連付けられている他のサイト間ピアが表示されます。これは、テーブルビューとグローバルビューに表示されます。

Security Cloud Control サイト間 VPN トンネルの削除

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **Network Connections** > **Site to Site VPN** をクリックして [VPN] ページを開きます。

ステップ 3 削除するサイト間 VPN トンネルを選択します。

ステップ 4 右側の [アクション（Actions）] ペインで、[削除（Delete）] をクリックします。

選択したサイト間 VPN トンネルが削除されます。

リモートアクセス仮想プライベートネットワークの概要

リモートアクセス仮想プライベートネットワーク（RA VPN）機能により、ユーザーは物理オフィス施設外の場所からネットワークに接続できます。これは、インターネットに接続されていて、ネットワークリソースに安全にアクセスできるコンピュータやサポートされている iOS/Android デバイスを使用できることを意味します。この機能は、データの安全性と保護を確保しながら、ホームネットワークまたはパブリック Wi-Fi ネットワークから接続する必要があるモバイルワーカーに特に役立ちます。

関連情報：

-
- FTD のリモートアクセス VPN を設定する

FDM 管理対象デバイスのリモートアクセス VPN の設定

Security Cloud Control は、新しいリモートアクセス仮想プライベートネットワーク（RA VPN）を設定するための直感的なユーザーインターフェイスを提供します。また、Security Cloud Control に搭載されている複数の FDM-managed デバイスの RA VPN 接続を迅速かつ簡単に設定できます。AnyConnect はエンドポイントデバイスでサポートされている唯一のクライアントで、FDM-managed デバイスへの RA VPN 接続が可能です。

AnyConnect クライアントが FDM-managed デバイスと SSL VPN 接続をネゴシエートする際、Transport Layer Security（TLS）または Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。クライアントおよび FDM-managed デバイスは、使用する TLS/DTLS バージョンをネゴシエートします。DTLS はクライアントがサポートする場合に使用されます。

Security Cloud Control は、FDM-managed デバイスでの RA VPN 機能の次の側面をサポートします。

- SSL クライアントベースのリモートアクセス
- IPv4 および IPv6 のアドレッシング
- 複数の FDM-managed デバイス間での共有 RA VPN 設定

重要 オンボード FDM-managed デバイス（ソフトウェアバージョン 6.7 以降で稼働）に SAML サーバーを認証ソースとして使用する RA VPN 設定が含まれている場合、Security Cloud Control は現在のリリースの SAML サーバーオブジェクトを管理しないため、接続プロファイルに AAA の詳細を入力しません。したがって、Security Cloud Control からはそのような RA VPN 設定を管理できません。ただし、Security Cloud Control は RA VPN 接続プロファイル、関連する信頼できる CA 証明書と SAML サーバーオブジェクトを読み取ります。

関連情報：

- RADIUS およびグループポリシーを使用したユーザーの権限および属性の制御 （66 ページ）
- FDM-Managed デバイス用のエンドツーエンドのリモートアクセス VPN 設定プロセス （84 ページ）
  - AnyConnect クライアント ソフトウェア パッケージのダウンロード （86 ページ）
  - バージョン 6.4.0 を実行している FDM-Managed デバイスへの AnyConnect ソフトウェアパッケージのアップロード （86 ページ）
  - バージョン 6.5 以降が実行されている FDM-Managed デバイスへの AnyConnect ソフトウェアパッケージのアップロード （90 ページ）
  - RA VPN AnyConnect クライアントプロファイルのアップロード （126 ページ）
  - FDM-Managed デバイスのアイデンティティソースの設定
    - アクティブ ディレクトリ レルム オブジェクトの作成または編集
    - RADIUS サーバーオブジェクトまたはグループの作成または編集
  - 新しい RA VPN グループポリシーの作成 （103 ページ）
  - RA VPN 設定の作成 （111 ページ）
  - RA VPN 接続プロファイルの設定 （116 ページ）
  - リモート アクセス VPN によるトラフィックの許可 （122 ページ）
  - バージョン 6.4.0 を実行している FDM-Managed デバイスの AnyConnect パッケージのアップグレード （123 ページ）
- FDM-Managed デバイスのリモートアクセス VPN のガイドラインと制限事項 （128 ページ）
- ユーザーが AnyConnect クライアントソフトウェアを FDM-Managed デバイスにインストールする方法 （129 ページ）
- リモート アクセス VPN のライセンス要件 （132 ページ）
- デバイス モデル別の同時 VPN セッションの最大数 （133 ページ）

RA VPN ユーザー用のスプリットトンネリング（ヘアピニング）

この記事では、RA VPN でのスプリットトンネリングについて説明します。

通常、リモートアクセス VPN では、VPN ユーザーに自社のデバイスを介してインターネットにアクセスさせます。ただし、RA VPN に接続している VPN ユーザーに、外部ネットワークへのアクセスを許可することができます。この技術は、スプリットトンネリングまたはヘアピニングと呼ばれます。スプリットトンネルでは、セキュアトンネル経由のリモートネットワークへの VPN 接続が可能ですが、VPN トンネル外のネットワークにも接続できます。スプリットトンネリングは、FTDデバイスのネットワーク負荷を軽減し、外部インターフェイスの帯域幅を拡大します。

スプリットトンネル リストを設定するには、標準アクセス リストまたは拡張アクセス リストを作成する必要があります。実行中のデバイスバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Virtual Private Networks (VPN)」の章にある「**How to Provide Internet Access on the Outside Interface for Remote Access VPN Users (Hair Pinning)**」セクションで説明されている手順に従ってください。

RADIUS およびグループポリシーを使用したユーザーの権限および属性の制御

ここでは、外部 RADIUS サーバーまたはグループポリシーから RA VPN 接続に属性を適用する方法について説明します。

外部 RADIUS サーバーまたは FDM-managed デバイスで定義されているグループポリシーから、RA VPN 接続にユーザーの認可属性（ユーザーの権利または権限とも呼ばれる）を適用できます。FDM-managedデバイスがグループポリシーに設定されている属性と競合する外部AAAサーバーから属性を受信した場合は、AAA サーバーからの属性が常に優先されます。

FDM-managed デバイスは次の順序で属性を適用します。

手順

ステップ 1 AAA サーバー上で定義されたユーザー属性：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。

ステップ 2 FDM-managedデバイス上で設定されているグループポリシー：RADIUSサーバーからユーザーのRADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場合は、FDM-managed

デバイスはそのユーザーを同じ名前のグループポリシーに入れて、そのグループポリシーの属性のうち、サーバーから返されないものを適用します。

ステップ 3 接続プロファイルによって割り当てられたグループポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザーに適用されるデフォルトのグループポリシーが含まれています。FDM-managedデバイスに接続するすべてのユーザーは、最初にこのグループに所属します。このグループでは、AAA サーバーから返されるユーザー属性、またはユーザーに割り当てられたグループ ポリシーにはない属性が定義されています。

FDM-managed デバイスは、ベンダー ID 3076 のRADIUS 属性をサポートします。使用するRADIUS サーバーにこれらの属性が定義されていない場合は、手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダーコード（3076）を使用します。

次のトピックでは、サポートされている属性値について、値がRADIUSサーバーで定義されるかどうか、またはRADIUSサーバーにシステムが送信する値であるかどうかに基づいて説明します。

RADIUS サーバーに送信された属性

RADIUS 属性 146 および 150 は、認証および許可の要求のために FDM-managed デバイスからRADIUS サーバーに送信されます。次の属性はすべて、アカウンティング開始、中間アップデート、および終了の要求の場合に FDM-managed デバイスから RADIUS サーバーに送信されます。

表 *1 : Secure Firewall Threat Defense* から *RADIUS* に送信される属性

属性（Attribute）	属性（Attribute）	構文、タイプ	シングルまたはマルチ値	説明または値
クライアント タイプ（Client Type）	150	整数	シングル	VPN に接続しているクライアントのタイプは次のとおりです。 2 = AnyConnect クライアント SSL VPN
セッション タイプ	151	整数	シングル	接続の種類： 1 = AnyConnect クライアント SSL VPN

属性（Attribute）	属性（Attribute）	構文、タイプ	シングルまたはマルチ値	説明または値
Tunnel Group Name	146	文字列	シングル	FDM-managed デバイスで定義されているセッションの確立に使用された接続プロファイルの名前。名前には 1 ～ 253 文字を使用できます。

RADIUS サーバーから受信した属性

次のユーザー認可属性が RADIUS サーバーから FDM-managed デバイスに送信されます。

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	86	文字列	シングル	両方の Access-List 属性で、FDM-managed デバイスで設定されている ACL の名前が使用されます。Smart CLI 拡張アクセスリストのオブジェクトタイプを使用して、それらの ACL を Firewall Device Manager で作成します（Firewall Device Manager にログインし、[デバイス（Device）] > [詳細設定（Advanced Configuration）] > [Smart CLI] > [オブジェクト（Objects）] を選択します）。これらの ACL は、着信（FDM-managed デバイスに入るトラフィック）または発信（FDM-managed デバイスから出るトラフィック）方向のトラフィックフローを制御します。
Access-List-Outbound	87	文字列	シングル	

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Address-Pools	217	文字列	シングル	FDM-managed デバイスで定義されたネットワークオブジェクトの名前。RA VPN へのクライアント接続のアドレスプールとして使用されるサブネットを識別します。[オブジェクト（Objects）] ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザーがログインしたときに表示されるバナー。
Banner2	36	文字列	シングル	ユーザーがログインするときに表示されるバナーの 2 番目の部分。Banner2 は Banner1 に付加されます。

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。RA VPN の[グループポリシー（Group Policy）]ページでグループポリシーを作成する必要があります。次の形式のいずれかを使用できます。 • グループ ポリシー名 • OU=グループポリシー名 • OU=グループポリシー名;
Simultaneous-Logins	2	整数	シングル	ユーザーが確立できる個別の同時接続数。0 ～ 2147483647。
VLAN	140	整数	シングル	ユーザーの接続を制限する VLAN。0 ～ 4094。FDM-managed デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

二要素認証

RA VPNの二要素認証を設定できます。二要素認証を使用する場合、ユーザーはユーザー名と静的パスワードに加えて、Duoパスコードなどの追加項目を指定する必要があります。二要素認証が 2 番目の認証ソースを使用することと異なるのは、1 つの認証ソースで 2 つの要素が設定され、Duo サーバーとの関係がプライマリ認証ソースに関連付けられている点です。Duo LDAPは例外で、Duo LDAP サーバーをセカンダリ認証ソースとして設定します。

• RADIUS を使用した Duo 二要素認証 （72 ページ）

• LDAP を使用した Duo 二要素認証 （77 ページ）

RADIUS を使用した Duo 二要素認証

Duo RADIUS サーバーはプライマリ認証ソースとして設定できます。このアプローチでは、Duo RADIUS 認証プロキシを使用します。

Duo の設定手順の詳細については、https://duo.com/docs/cisco-firepower を参照してください。

その後、最初の認証要素として別の RADIUS サーバーまたは Microsoft Active Directory（AD）サーバーを使用し、2 番目の要素として Duo クラウドサービスを使用するため、プロキシサーバー宛の認証要求を転送するように Duo を設定します。

このアプローチを使用する場合、ユーザーは、Duo 認証プロキシおよび関連する RADIUS/AD サーバーの両方で設定されているユーザー名と、RADIUS/AD サーバーで設定されたユーザー名のパスワード（その後に次のいずれかの Duo コードが続く）を使用して認証する必要があります。

Duo-passcode。my-password,12345 など

push。たとえば、*my-password*,**push** など。**push** は、ユーザーによるインストールと登録が完了している Duo モバイルアプリに認証をプッシュ送信するように Duo に指示する場合に使用します。

SMS。たとえば、*my-password*,**sms** など。sms は、ユーザーのモバイルデバイスにパスコードの新しいバッチと SMS メッセージを送信するように Duo に指示する場合に使用します。sms を使用すると、ユーザーの認証試行は失敗します。ユーザーは再認証し、2 番目の要素として新しいパスコードを入力する必要があります。

電話。*my-password*,**phone** など。phone は、電話コールバック認証を実行するように Duo に指示する場合に使用します。

ユーザー名とパスワードが認証されると、Duo 認証プロキシは Duo クラウドサービスに接続し、Duo クラウドサービスは、その要求が設定されている有効なプロキシデバイスからのものであることを検証してから、指示に従ってユーザーのモバイルデバイスに一時的なパスコードをプッシュ送信します。ユーザーがこのパスコードを受け入れると、セッションは Duo で認証済みとマークされ、RA VPN が確立されます。

詳細な説明については、Duo RADIUS を使用した二要素認証の設定方法 （72 ページ）を参照してください。

Duo RADIUS を使用した二要素認証の設定方法

Duo RADIUS サーバーはプライマリ認証ソースとして設定できます。このアプローチでは、Duo RADIUS 認証プロキシを使用します。

その後、最初の認証要素として別の RADIUS サーバー（または AD サーバー）を使用し、2 番目の要素として Duo クラウド サービスを使用するため、プロキシ サーバー宛の認証要求を転送するように Duo を設定します。

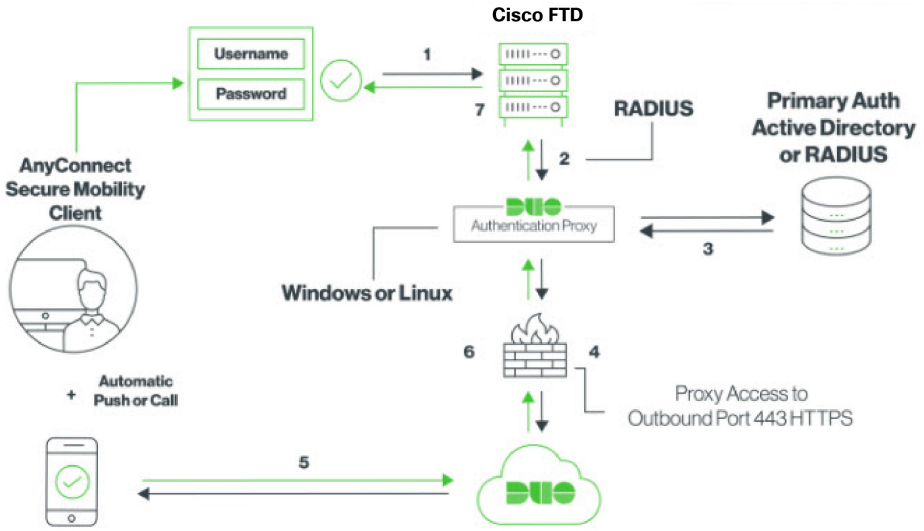
以降のトピックでは設定についてさらに詳しく説明します。

• Duo RADIUS セカンダリ認証のシステムフロー （73 ページ）

• Security Cloud Control を使用した Duo RADIUS のデバイスの設定 （74 ページ）

Duo RADIUS セカンダリ認証のシステムフロー

次に、システムフローについて説明します。



1. ユーザーはFDM-managedデバイスへのリモートアクセスVPN接続を確立し、RADIUS/ADサーバーに関連付けられたユーザー名、RADIUS/AD サーバーで設定されたユーザー名のパスワード、いずれかの DUO コード（Duo パスワード、プッシュ、SMS、または電話番号）を指定します。詳細については、RADIUS を使用した Duo 二要素認証 （72 ページ）
2. FDM-managed デバイスは、認証要求を Duo Authentication Proxy に送信します。
3. Duo Authentication Proxy は、プライマリ認証サーバー（Active Directory や RADIUS など）でプライマリ認証の試行を認証します。
4. ログイン情報が認証されると、Duo Security への Duo Authentication Proxy 接続が TCP ポート 443 経由で確立されます。
5. 要求を受けたDuoは、プッシュ通知、パスコード付きのテキストメッセージ、または電話コールによって、ユーザーを個別に認証します。ユーザーはこの認証を正常に完了する必要があります。
6. Duo Authentication Proxy が認証応答を受信します。
7. セカンダリ認証が成功すると、FDM-managed デバイスは、ユーザーの AnyConnect クライアントとのリモートアクセス VPN 接続を確立します。

Duo RADIUS セカンダリ認証の設定

Duo Authentication Proxy は、プライマリ認証サーバー（Active Directory や RADIUS など）でプライマリ認証の試行を認証します。

Duo アカウントの作成

Duo アカウントを作成し、統合鍵、秘密鍵、および API ホスト名を取得します。

次に、プロセスの概要を示します。詳細については、Duo の Web サイトを参照してください。

手順

ステップ 1 Duo アカウントにサインアップします。

ステップ 2 Duo Admin Panel にログインし、[アプリケーション（Applications）] に移動します。

ステップ 3 [アプリケーションの保護（Protect an Application）] をクリックし、アプリケーションリストで **Cisco Firepower Threat Defense VPN** を探します。

ステップ 4 [アプリケーションの保護（Protect this Application）] をクリックし、統合鍵、秘密鍵、および API ホスト名を取得します。この情報は、プロキシを設定するときに必要になります。詳細については、*Duo Getting Started* ガイド（https://duo.com/docs/getting-started）を参照してください。

ステップ 5 Duo Authentication Proxy をインストールして設定します。手順については、https://duo.com/docs/cisco-firepower の「Install the Duo Authentication Proxy」を参照してください。

ステップ 6 認証プロキシを開始します。手順については、https://duo.com/docs/cisco-firepower の「Start the Proxy」を参照してください。

Duo に新しいユーザーを登録する手順については、https://duo.com/docs/enrolling-users を参照してください。

Security Cloud Control を使用した Duo RADIUS のデバイスの設定

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 FTD RADIUS サーバーオブジェクトを設定します。

a) 左側のペインで **Objects** をクリックします。

b)  > [RA VPNオブジェクト（Cisco ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [アイデンティティソース（Identity Source）] をクリックします。

c) 名前を指定し、[デバイスタイプ（Device Type）] を [FTD] に設定します。

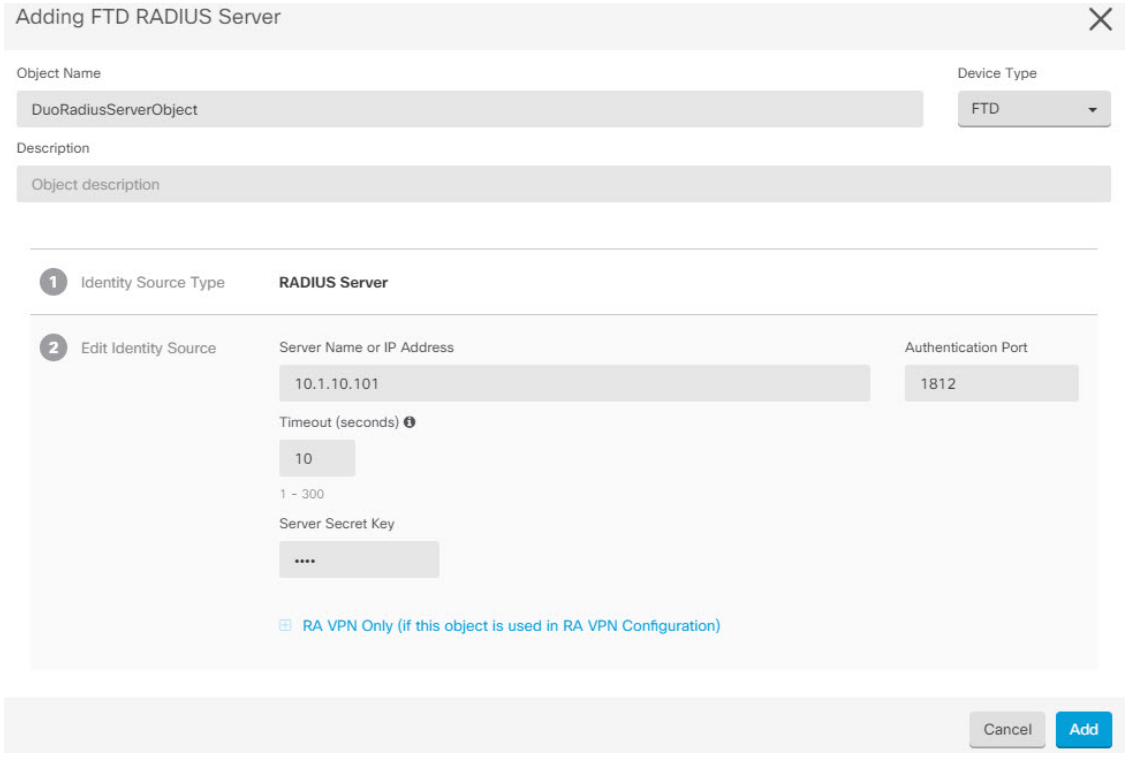
d) [RADIUSサーバーグループ（Radius Server Group）] を選択し、[続行（Continue）] をクリックします。

詳細については、RADIUS サーバーグループの作成のステップ 6 を参照してください。

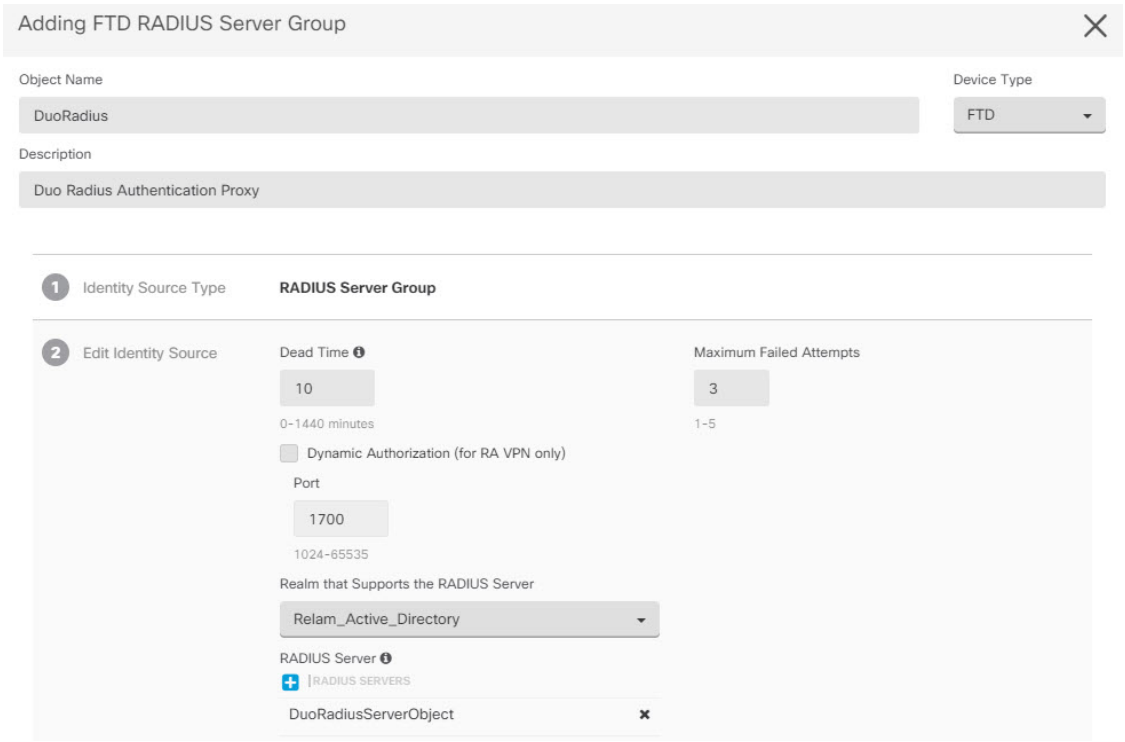
e) [RADIUSサーバー（Radius Server）] セクションで、[追加（Add）] ボタンをクリックし、[新しいRADIUSサーバーの作成（Create New Radius Server）] をクリックします。

RADIUS サーバーオブジェクトの作成を参照してください。

[サーバー名またはIPアドレス（Server Name or IP Address）] フィールドに Duo Authentication Proxy サーバーの完全修飾ホスト名か IP アドレスを入力します。



f) Duo RADIUS サーバーをグループに追加したら、[追加（Add）] をクリックして新しい Duo RADIUS サーバーグループを作成します。



ステップ 3 [リモートアクセスVPN認証方式（Remote Access VPN Authentication Method）] を [Duo RADIUS] に変更します。

a) 左側のペインで **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM** をクリックします。

b) VPN の設定を展開し、Duo を追加する接続プロファイルをクリックします。

c) 右側の [アクション（Actions）] ペインで、[編集（Edit）] をクリックします。

d) [認証タイプ（Authentication Type）]（[AAA] または [AAAとクライアント証明書（AAA and Client Certificate）]）のいずれかを選択します。

e) [ユーザー認証用のプライマリIDソース（Primary Identity Source for User Authentication）] リストで、以前作成したサーバーグループを選択します。

f) 通常は [承認サーバー（Authorization Server）] や [アカウンティングサーバー（Accounting Server）] を選択する必要はありません。

g) [続行（Continue）] をクリックします。
h) [概要と手順（Summary and Instructions）] のステップで、[完了（Done）] をクリックして設定を保存します。

ステップ 4 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

LDAP を使用した Duo 二要素認証

プライマリソースとしての Microsoft Active Directory（AD）または RADIUS サーバとともに、セカンダリ認証ソースとして Duo LDAP サーバを使用できます。Duo LDAP を使用すると、セカンダリ認証により、プライマリ認証が Duo パスコード、プッシュ通知、または電話コールで検証されます。

（注） Duo の 二要素認証機能は、Firepower Threat バージョン 6.5 以降を実行しているデバイスに対して Security Cloud Control で使用できます。

FDM-managed デバイスは、ポート TCP/636 経由で LDAPS を使用して、Duo LDAP と通信します。

このアプローチを使用する場合は、AD/RADIUS サーバと Duo LDAP サーバの両方で設定されているユーザ名を使用して認証する必要があります。AnyConnect によってログインするように求められた場合は、プライマリ [パスワード（Password）] フィールドに AD/RADIUS のパスワードを入力します。[セカンダリパスワード（Secondary Password）]では、次のいずれかを使用して Duo で認証します。詳細については、https://guide.duo.com/anyconnect の「要素選択用の 2 つ目のパスワード」セクションを参照してください。

- [Duoパスコード（Duo passcode）]：Duo Mobile で生成され、SMS を介して送信され、ハードウェア トークンによって生成されるパスコード、または管理者によって提供されるパスコードを使用して、認証します。1234567 などです。
- [プッシュ（push）]：Duo Mobile アプリをインストールしてアクティブにしている場合は、ログイン要求を電話機にプッシュします。要求を確認し、[承認（Approve）] をタップしてログインします。
- [電話（phone）]：電話機のコールバックを使用して認証します。
- [sms]：Duo パスコードをテキストメッセージで要求します。ログイン試行は失敗します。新しいパスコードを使用して再度ログインします。

詳細な説明については、Duo LDAP を使用した二要素認証の設定方法 （77 ページ）を参照してください。

Duo LDAP を使用した二要素認証の設定方法

プライマリソースとしての Microsoft Active Directory（AD）または RADIUS サーバとともに、セカンダリ認証ソースとして Duo LDAP サーバを使用できます。Duo LDAP を使用すると、セ

カンダリ認証により、プライマリ認証がDuoパスコード、プッシュ通知、または電話コールで検証されます。

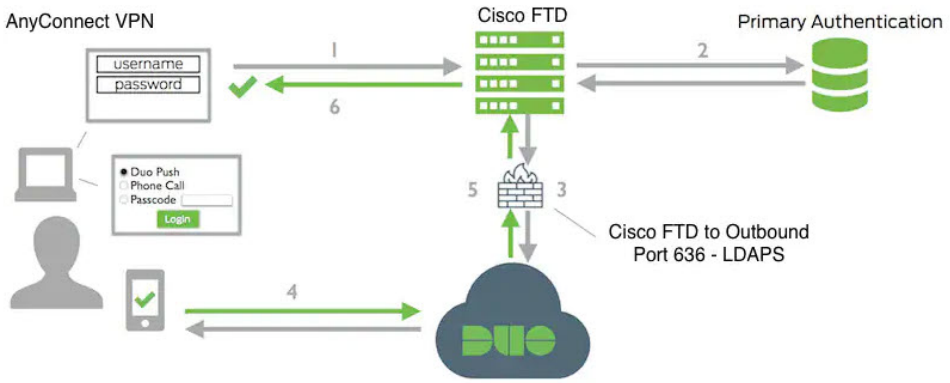
以降のトピックでは設定についてさらに詳しく説明します。

- Duo LDAP セカンダリ認証のシステム フロー （78 ページ）
- Duo LDAP セカンダリ認証の設定 （78 ページ）

Duo LDAP セカンダリ認証のシステム フロー

次の図は、LDAP を使用した二要素認証を実現するために、Firewall Threat Defense と Duo がどのように連携するかを示しています。

次に、システムフローについて説明します。



1. ユーザーは、FDM-managed デバイスへのリモートアクセス VPN 接続を確立し、ユーザー名とパスワードを提供します。
2. FDM-managed デバイスは、プライマリ認証サーバー（Active Directory や RADIUS など）でプライマリ認証の試行を認証します。
3. プライマリ認証が機能する場合、FDM-managedデバイスはDuo LDAP サーバーにセカンダリ認証の要求を送信します。
4. 要求を受けたDuoは、プッシュ構成、パスコード付きのテキストメッセージ、または電話コールによって、ユーザーを個別に認証します。ユーザーはこの認証を正常に完了する必要があります。
5. Duo は FDM-managed デバイスに応答して、ユーザーが正常に認証されたかどうかを示します。
6. セカンダリ認証が成功すると、FDM-managed デバイスは、ユーザーの AnyConnect クライアントとのリモートアクセス VPN 接続を確立します。

Duo LDAP セカンダリ認証の設定

次の手順では、セカンダリ認証ソースとして Duo LDAP を使用して、リモートアクセス VPN の二要素認証を設定するエンドツーエンドのプロセスについて説明します。この設定を完了するには、Duo のアカウントを取得し、Duo から情報を取得する必要があります。

Duo アカウントの作成

Duo アカウントを作成し、統合鍵、秘密鍵、および API ホスト名を取得します。

次に、プロセスの概要を示します。詳細については、Duo の Web サイトを参照してください。

手順

ステップ 1 Duo アカウントにサインアップします。

ステップ 2 Duo Admin Panel にログインし、[アプリケーション（Applications）] に移動します。

ステップ 3 [アプリケーションの保護（Protect an Application）] をクリックし、アプリケーションリストで **Cisco Firepower Threat Defense VPN** を探します。

ステップ 4 [アプリケーションの保護（Protect this Application）] をクリックして、**統合鍵**、**秘密鍵**、および **API ホスト名**を取得します。詳細については、*Duo Getting Started*（https://duo.com/docs/getting-started）を参照してください。

Duo に新しいユーザーを登録する手順については、https://duo.com/docs/enrolling-users を参照してください。

FDM-Managed デバイスへの信頼できる CA 証明書のアップロード

FDM-managed デバイスには、Duo LDAP サーバーへの接続を検証するために必要な、信頼できる CA 証明書が必要です。https://www.digicert.com/digicert-root-certificates.htm に直接アクセスし、**DigiCertSHA2HighAssuranceServerCA** または **DigiCert High Assurance EV Root CA** をダウンロードし、Firewall Device Manager（FDM）を使用してアップロードできます。

手順

ステップ 1 FDM-managed デバイスの Firewall Device Manager ページにアクセスし、[オブジェクト（Objects）] > [証明書（Certificates）] の順に選択します。

ステップ 2 [+] > [信頼できる CA の証明書の追加（Add Trusted CA Certificate）] をクリックします。

ステップ 3 証明書の名前を入力します（例：DigiCert_High_Assurance_EV_Root_CA）(スペースは使用できません)。

ステップ 4 [証明書のアップロード（Upload Certificate）] をクリックし、ダウンロードしたファイルを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 デバイスをまだオンボードしていない場合は、Security Cloud Control にオンボードします。

ステップ 7 FTD から Security Cloud Control への設定変更を読み取ります。

Security Cloud Control での Duo LDAP 用 FTD の設定

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 Duo LDAP サーバーの Duo LDAP アイデンティティ ソース オブジェクトを作成します。

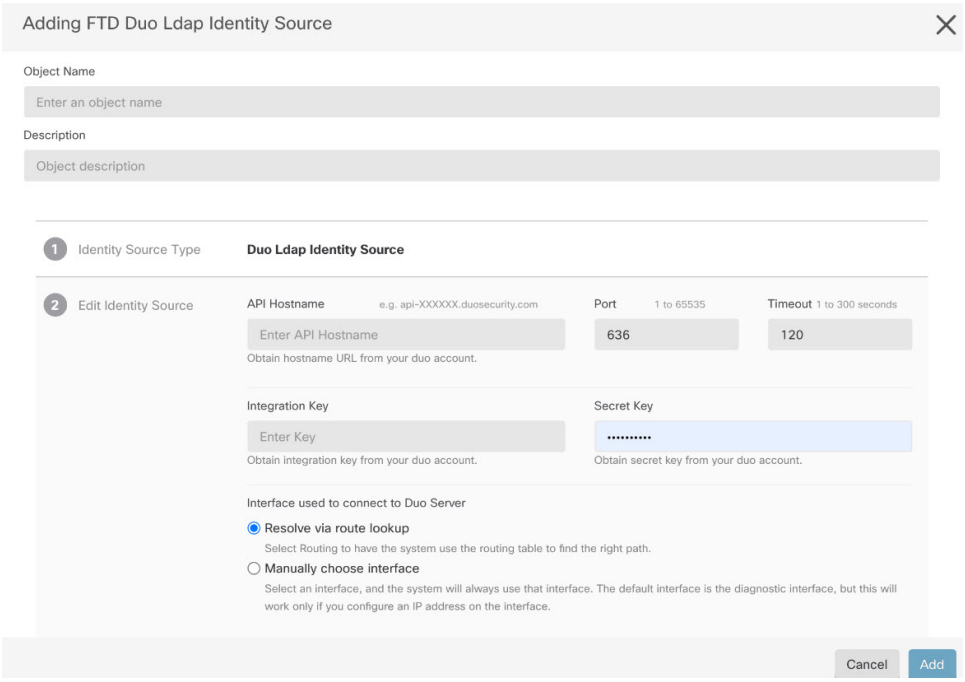
a) 左側の Security Cloud Control ナビゲーションバーで、**Objects** をクリックします。

b)  > [RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [アイデンティティソース（Identity Source）] をクリックしてオブジェクトを作成します。

c) オブジェクトの名前（Duo-LDAP-server など）を入力します。

d) [デバイスタイプ（Device Type）] として [FTD] を選択します。

e) [Duo LDAPアイデンティティソース（Duo LDAP Identity Source）] をクリックして、[続行（Continue）] をクリックします。



f) [アイデンティティソースの編集（Edit Identity Source）] 領域で、次の詳細を指定します。

- [APIホスト名（API Hostname）] には、Duo アカウントから取得した API ホスト名を入力します。ホスト名は API-XXXXXXXX.DUOSECURITY.COM のような形式になります。X を一意の値に置き換えます。大文字は必須ではありません。

- [ポートPort] には、LDAPS に使用する TCP ポートを入力します。Duo から別のポートを使用するように指示されていない限り、この値は 636 になります。アクセス制御リストで、必ずこのポートを介した Duo LDAP サーバーへのトラフィックを許可してください。
- [タイムアウト（Timeout）]：Duo サーバーに接続する際のタイムアウトを秒単位で入力します。値は 1 ー 300 秒です。デフォルトは 120 です。デフォルトを使用するには、120 を入力するか、属性行を削除します。
- [統合鍵（Integration Key）]：Duo アカウントから取得した統合鍵を入力します。
- [秘密鍵（Secret Key）]：Duo アカウントから取得した秘密鍵を入力します。この鍵はその後マスクされます。
- [Duoサーバーへの接続に使用するインターフェイス（Interface used to connect to Duo Server）]：Duo サーバーへの接続に使用するインターフェイスを選択します。
  - [ルートルックアップ経由で解決する（Resolve via Route Lookup）]：ルーティングテーブルを使用して正しいパスを見つけるには、このオプションを選択します。ルーティングテーブルの作成については、「ルーティング」を参照してください。
  - [インターフェイスを手動で選択する（Manually Choose Interface）]：このオプションを選択し、リストからいずれかのインターフェイスを選択します。デフォルトのインターフェイスは診断インターフェイスですが、これはインターフェイスで IP アドレスを設定する場合にのみ動作します。注：選択したインターフェイスが、Duo サーバーに接続するデバイスに存在することを確認してください。
  - [追加（Add）] をクリックします。

ステップ 3 （オプション）AnyConnect プロファイルエディタを使用して、 60 秒以上の認証タイムアウトを指定するプロファイルを作成します。

ユーザーが Duo のパスコードを取得し、セカンダリ認証を完了できるように、指定する時間に余裕を持たせる必要があります。60 秒以上を推奨します。次の手順では、認証タイムアウトのみを設定してから、FDM-managed デバイスにプロファイルをアップロードする方法について説明します。他の設定を変更する場合は、ここで行ってください。

a) AnyConnectプロファイルエディタパッケージをダウンロードしてインストールします（まだ行っていない場合）。このパッケージは、Cisco Software Center（software.cisco.com）の使用している AnyConnect バージョンのフォルダにあります。このマニュアルの執筆時点におけるベースパスは、[ダウンロードホーム（Downloads Home）] > [セキュリティ（Security）] > [VPNおよびエンドポイントセキュリティクライアント（VPN and Endpoint Security Clients）] > [Cisco VPNクライアント（Cisco VPN Clients）] > [AnyConnectセキュアモビリティクライアント（AnyConnect Secure Mobility Client）] です。
b) [AnyConnect VPNプロファイルエディタ（AnyConnect VPN Profile Editor）] を開きます。
c) 目次の [設定（パート2）（Preferences (Part 2)）] を選択し、ページの最後までスクロールして、[認証タイムアウト（Authentication Timeout）] を 60 以上に変更します。次の図は

AnyConnect 4.7 VPN プロファイルエディタからの引用です。それより前のバージョンや後のバージョンでは、内容が異なる場合があります。

d) [ファイル（File）] > [保存（Save）] を選択し、プロファイル XML ファイルに適切な名前（duo-ldap-profile.xml など）を付けてワークステーションに保存します。

e) これで、**VPN プロファイル エディタ** アプリケーションを閉じることができます。

f) Security Cloud Control で「RA VPN AnyConnect クライアントプロファイルのアップロード」を実行します。

ステップ 4 グループポリシーを作成し、ポリシーで AnyConnect プロファイルを選択します。

ユーザーに割り当てるグループポリシーは、接続のさまざまな側面を制御します。次の手順では、プロファイル XML ファイルをグループに割り当てる方法について説明します。詳細については、「新しい FTD RA VPN グループポリシーの作成」を参照してください。

a) 左側の Security Cloud Control ナビゲーションバーで、**Objects** をクリックします。

b) 既存のグループポリシーを編集するには、[RA VPNグループポリシー（RA VPN Group Policy）] フィルタを使用して既存のグループポリシーのみを表示し、必要なポリシーを変更して保存します。

c) 新しいグループポリシーを作成するには、[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [RA VPNグループポリシー（RA VPN Group Policy）] をクリックします。

d) [全般（General）] ページで、次のプロパティを設定します。

- [名前（Name）]：新しいプロファイルの場合は、名前を入力します。たとえば、Duo-LDAP-group と入力します。
- [AnyConnectクライアントプロファイル（AnyConnect Client Profiles）]：作成した AnyConnect クライアントプロファイルを選択します。

e) [追加（Add）] をクリックして、オブジェクトを保存します。

f) **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM** をクリックします。

g) 更新するリモートアクセス VPN の設定をクリックします。

h) 右側の [操作（Actions）] ウィンドウで、[グループポリシー（Group Policies）] をクリックします。

i) [+] をクリックして、VPN 設定に関連付けるグループポリシーを選択します。

j) [保存（Save）] をクリックして、グループポリシーを保存します。

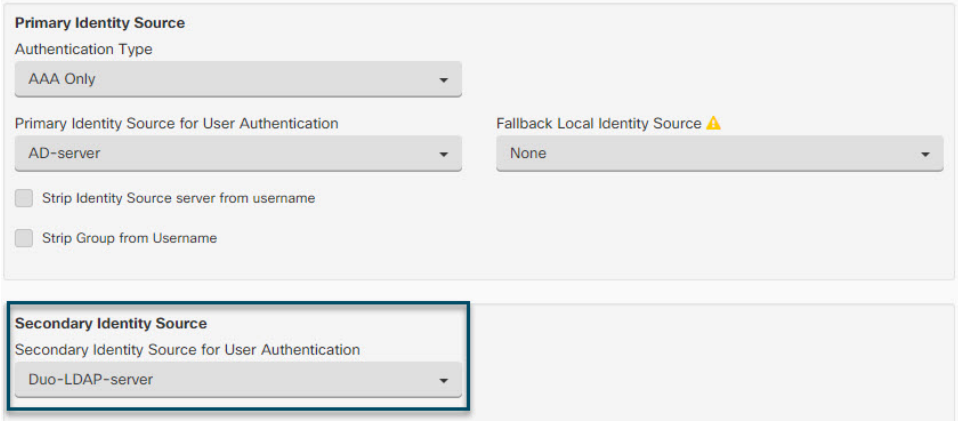
ステップ 5 Duo LDAP セカンダリ認証に使用するリモートアクセス VPN 接続プロファイルを作成または編集します。

次の手順では、Duo LDAP をセカンダリ認証ソースとして有効にし、AnyConnect クライアントプロファイルを適用するための主な変更について説明します。新しい接続プロファイルの場合は、残りの必須フィールドも設定する必要があります。この手順では、既存の接続プロファイルを編集しており、これら 2 つの設定のみを変更する必要があると仮定しています。

a) Security Cloud Control ナビゲーションページで、[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）] をクリックします。

b) リモートアクセス VPN の設定を展開し、更新する接続プロファイルをクリックします。
c) 右側の [操作（Actions）] ウィンドウで、[編集（Edit）] をクリックします。
d) [プライマリアイデンティティソース（Primary Identity Source）] で、次を設定します。

- [認証タイプ（Authentication Type）]：[AAAのみ（AAA Only）] または [AAAとクライアント証明書（AAA and Client Certificate）] のいずれかを選択します。AAA を使用していない場合、二要素認証を設定できません。
- [ユーザー認証のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：プライマリ Active Directory または RADIUS サーバーを選択します。プライマリソースとして Duo-LDAP アイデンティティソースを選択できることに注意してください。ただし、Duo-LDAP は認証サービスのみを提供し、アイデンティティサービスは提供しないため、プライマリ認証ソースとして Duo-LDAP を使用する場合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザー名は表示されず、これらのユーザーに対してアクセス制御ルールを作成することはできません（必要に応じて、ローカル アイデンティティ ソースへのフォールバックを設定できます）。
- [セカンダリアイデンティティソース（Secondary Identity Source）]：Duo-LDAP のアイデンティティソースを選択します。



（注）
[プライマリアイデンティティソース（Primary Identity Source）] と [セカンダリアイデンティティソース（Secondary Identity Source）] のユーザー名が同じ場合は、接続プロファイルの [詳細（Advanced）] オプションで、[セカンダリログインにプライマリユーザー名を使用（Use Primary Username for Secondary Login）] を有効にすることをお勧めします。このように設定すると、エンドユーザーは、プライマリとセカンダリの両方のアイデンティティソースに単一のユーザー名を使用できます。

e) [続行（Continue）] をクリックします。

f) [グループポリシー（Group Policy）]ページで、作成または編集したグループポリシーを選択します。

g) [続行（Continue）] をクリックします。

h) [完了（Done）] をクリックして、接続プロファイルへの変更を保存します。

ステップ 6 すべてのデバイスの設定変更のプレビューと展開。

FDM-Managed デバイス用のエンドツーエンドのリモートアクセス VPN 設定プロセス

ここでは、Security Cloud Control にオンボードされた FDM-managed デバイスでリモートアクセス仮想プライベートネットワーク（RA VPN）を設定するためのエンドツーエンドの手順について説明します。

クライアントのリモートアクセス VPN を有効化するには、いくつかの異なる項目を設定する必要があります。次の手順では、エンドツーエンドのプロセスについて説明します。

手順

ステップ 1 2 つのライセンスを有効にします。

- デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager アカウントによってエクスポートを制御する必要があります。リモートアクセス VPN を設定するには、ライセンスが輸出規制要件を満たしている必要があります。また、評価ライセンスを使用して機能を設定することはできません。FDM-managed デバイスを購入すると、ライセンスが自動的に含まれます。ライセンスは、オプションライセンスではカバーされないすべての機能をカバーしています。これは永久ライセンスです。デバイスは Secure Firewall Device Managerに登録されている必要があります。デバイスで実行しているバージョンの Cisco Secure Firewall Threat Defense コンフィギュレーション ガイド[英語] の「Licensing the System」の章にある「Registering the Device」を参照してください。
https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html
- ライセンス。詳細については、「リモートアクセス VPN のライセンス要件」を参照してください。
  - ライセンスを有効にするには、デバイスで実行しているバージョンの Cisco Secure Firewall Threat Defense コンフィギュレーション ガイド[英語] の「Licensing the System」の章にある「Enabling or Disabling Optional Licenses」を参照してください。
https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

ステップ 2 証明書を設定します。

証明書は、クライアントとデバイスの間の SSL 接続を認証するために必要です。VPN 用の事前定義された DefaultInternalCertificate を使用できます。または、独自に作成できます。

認証に使われるディレクトリ レルムに暗号化接続を使用する場合は、信頼される CA 証明書をアップロードする必要があります。証明書、および証明書のアップロード方法の詳細については、「証明書の設定」を参照してください。

ステップ 3 リモート ユーザを認証する目的で使用されるアイデンティティ ソースを設定します。

次のソースを使用して、RA VPN を使用してネットワークに接続しようとするユーザーを認証できます。さらに、クライアント証明書を単独で、またはアイデンティティソースと連携させて、認証に使用できます。

- Active Directory アイデンティティレルム：プライマリ認証ソースとして使用できます。ユーザ アカウントは Active Directory（AD）サーバで定義されます。「AD アイデンティティレルムの設定」を参照してください。「Active Directory レルムオブジェクトの作成または編集」を参照してください。
- RADIUS サーバーグループ：プライマリまたはセカンダリ認証ソースとして使用でき、認可およびアカウンティングに使用できます。「RADIUS サーバーオブジェクトまたはグループの作成または編集」を参照してください。
- ローカル ID ソース（ローカル ユーザー データベース）：プライマリ ソースまたはフォールバック ソースとして使用できます。デバイスで直接ユーザを定義できます。外部サーバを使用することはできません。フォールバック ソースとしてローカルデータベースを使用する場合は、必ず外部サーバーで定義したものと同じユーザー名/パスワードを定義します。

  （注）
  Secure Firewall Device Manager からのみ FDM-managed デバイスに直接ユーザーアカウントを作成できます。「ローカルユーザーの設定」を参照してください。

ステップ 4 （オプション）新しい RA VPN グループポリシーを作成します。

グループポリシーは、ユーザーに関連する属性を定義します。グループメンバーシップに基づいて、リソースへの差分アクセスを提供するためにグループポリシーを設定することができます。または、すべての接続でデフォルトポリシーを使用します。

ステップ 5 RA VPN 設定を作成します。

ステップ 6 RA VPN 接続プロファイルを設定します。

ステップ 7 設定の変更を確認して、デバイスに展開します。

ステップ 8 リモートアクセス VPN によるトラフィックを許可します。

ステップ 9 （オプション）アイデンティティ ポリシーを有効にして、パッシブ認証のルールを設定します。パッシブ ユーザ認証を有効にすると、リモート アクセス VPN 経由でログインするユーザがダッシュボードに表示され、ポリシー内のトラフィック一致基準としても使用できます。パッシブ認証を有効にしない場合、RA VPN ユーザはアクティブ認証ポリシーに一致する場合にのみ使用できます。ダッシュボードのユーザー情報またはトラフィック照合用のユーザー情

報を取得するには、アイデンティティ ポリシーを有効にする必要があります。「ID ポリシーの設定」を参照してください。

重要 Secure Firewall Device Manager などのローカルマネージャーを使用してリモートアクセス VPN の設定を変更すると、Security Cloud Control では、そのデバイスの [設定ステータス（Configuration Status）] に [競合検出（Conflict Detected）] と表示されます。「FDM-Managed デバイスでのアウトオブバンド変更」を参照してください。この FDM-managed デバイスで設定の競合を解決できます。

次のタスク

RA VPN 設定が FDM-managed デバイスにダウンロードされると、ユーザーは、インターネットに接続されているコンピュータやその他のサポートされている iOS または Android デバイスを使用して、リモートの場所からネットワークに接続できます。テナント内のすべてのオンボード RA VPN ヘッドエンドから、ライブ AnyConnect リモートアクセス仮想プライベートネットワーク（RA VPN）セッションを監視できます。

「リモートアクセス仮想プライベートネットワークの監視」を参照してください。

AnyConnect クライアント ソフトウェア パッケージのダウンロード

リモートアクセス VPN を設定する前に、https://software.cisco.com/download/home/283000185 から AnyConnect ソフトウェアパッケージをワークステーションにダウンロードする必要があります。必要なオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」をダウンロードしていることを確認してください。後で、VPN を定義するときに、これらのパッケージを Firepower Threat Defense（FTD）デバイスにアップロードできます。

最新の機能、バグ修正、セキュリティパッチを確保するには、常に最新の AnyConnect バージョンをダウンロードする必要があります。デバイスのパッケージは定期的に更新してください。

（注） オペレーティングシステム（OS）（Windows、Mac、Linux）ごとに 1 つの AnyConnect をアップロードできます。1 つの OS タイプに対して複数のバージョンをアップロードすることはできません。

バージョン 6.4.0 を実行している FDM-Managed デバイスへの AnyConnect ソフトウェアパッケージのアップロード

Firewall Device Manager API エクスプローラを使用して、バージョン 6.4.0 を実行している FDM-managed デバイスに AnyConnect ソフトウェアパッケージをアップロードできます。RA VPN 接続を作成するには、デバイスに少なくとも 1 つの AnyConnect ソフトウェアパッケージが存在する必要があります。

重要 この手順は、Firewall Device Manager バージョン 6.4 にのみ当てはまります。Firewall Device Manager バージョン 6.5 以降を使用している場合は、Security Cloud Control インターフェイスを使用して AnyConnect パッケージをアップロードします。

次の手順を使用して、AnyConnect パッケージを Firewall Device Manager バージョン 6.4.0 にアップロードします。

手順

ステップ 1 https://software.cisco.com/download/home/283000185 から AnyConnect パッケージをダウンロードします。

- EULA に同意し、K9（暗号化されたイメージ）の権限を持っていることを確認してください。
- 使用しているオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」を選択します。パッケージ名は「anyconnect-win-4.7.04056-webdeploy-k9.pkg」のようになります。Windows、macOS、Linux それぞれに向けたヘッドエンド Web 展開パッケージがあります。

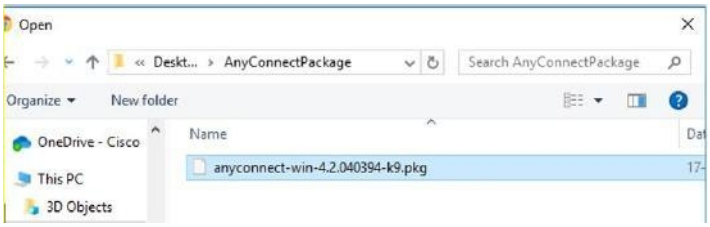
ステップ 2 ブラウザを使用して、システムのホームページを開きます。例：https://ftd.example.com。

ステップ 3 Firewall Device Manager にログインします。

ステップ 4 /#/Api-explorer を指すように URL を編集します（たとえば、https://ftd.example.com/#/api-explorer）。

ステップ 5 下にスクロールして、**[アップロード（Upload）]** > **[/action/uploaddiskfile]** をクリックします。

ステップ 6 [fileToUpload] フィールドで [ファイルの選択（Choose File）] をクリックして、必要な AnyConnect パッケージを選択します。複数のパッケージを一度にアップロードできます。



ステップ 7 [開く（Open）] をクリックします。

ステップ 8 下にスクロールして、[試す（TRY IT OUT!）] をクリックします。 パッケージが完全にアップロードされるまで待ちます。[応答本文（Response Body）] には、API 応答が次の形式で表示されます。

```
{ "version": null, "name": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"fileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"id": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
```

"type": "fileuploadstatus",
"links": {
"self":

https://ftd.example.com:972/api/fdm/...90d111e9-a361- cf32937ce0df.pkg

} }

応答からパッケージの **fileName** を記録します。POST 操作を実行するときに、この文字列を入力する必要があります。この例では、fileName は **691f47e1-90c7-11e9-a361-79e2452f0c57.pkg** です。

ステップ 9 Firewall Threat Defense REST API ページの上部近くまでスクロールして、**[AnyConnectPackageFile]** > **[POST /object/anyconnectpackagefiles]** をクリックします。API に対して POST 操作を実行し、パッケージファイルの一時的にステージングされた diskFilename と OS タイプをペイロードで指定します。このアクションにより、AnyConnect パッケージファイルが作成されます。

ステップ 10 **body** フィールドに、パッケージの詳細を次の形式でのみ入力します。

{ "platformType": "WINDOWS",
"diskFileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"type": "anyconnectpackagefile",
"name": "AnyConnectWindowsBGL" }

1. **platformType** フィールドに、OS プラットフォームを WINDOWS、MACOS、または LINUX として入力します。
2. **diskFileName** フィールドに、ディスクファイルのアップロード後に記録した **fileName** を入力します。
3. **name** フィールドに、パッケージに設定する名前を入力します。
4. [試す（TRY IT OUT!）] をクリックします。

   [応答本文（Response Body）] フィールドには、POST が正常に動作した後に API 応答が次の形式で表示されます。

{ "version": "ni7xeneslft3p",
"name": "AnyConnectWindowsBGL" }
"description": null,
"diskFileName": "41d592e3-90ca-11e9-a361-6d05320a165d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": { "self":

"https:/>/ftd.example.com:972...1-cf32937ce0df"

}
}

AnyConnect パッケージが Firewall Device Manager に作成されます。

ステップ 11 **[AnyConnectPackageFile]** > **[GET /object/anyconnectpackagefiles]** > **[試す（TRY IT OUT!）]** をクリックします。

[応答本文（Response Body）] に、すべての AnyConnect パッケージファイルが表示されます。

応答の例を次に示します。


```
{
"items": [
{
"version": "la4nwceqk2sg4",
"name": "AnyConnectWindowsBGL" }
"description": null,
"diskFileName": "82f1e362-9cd8-11e9-a361-9758ba07962d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": {
"self":
"https://ftd.example.com:972...1-23534f081c43"
}
}
],
```


ステップ 12 OS タイプごとに他の AnyConnect パッケージをアップロードします。手順 4 から 10 を繰り返します。

ステップ 13 Web ページをポイントするように URL を編集します（例：https://ftd.example.com）。https://ftd.example.com/#/api-explorer

ステップ 14 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。このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

ステップ 15 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。

（注） FDM-managed デバイスからパッケージを削除するには、**[AnyConnectPackageFile]** > **[削除（Delete）]** をクリックします。[objID] フィールドにパッケージ ID を入力し、[試す（TRY IT OUT!）] をクリックします。

VPN 接続を完了するには、ユーザーは AnyConnect クライアントソフトウェアをワークステーションにインストールする必要があります。詳細については、ユーザーが AnyConnect クライ

アントソフトウェアを FDM-Managed デバイスにインストールする方法 （129 ページ）を参照してください。

バージョン 6.5 以降が実行されている FDM-Managed デバイスへの AnyConnect ソフトウェアパッケージのアップロード

RA VPN を設定するために、バージョン 6.5 以降を実行している FDM-managed デバイスを使用している場合は、Security Cloud Control の RA VPN ウィザードを使用して AnyConnect ソフトウェアパッケージをデバイスにアップロードできます。RA VPN ウィザードでは、AnyConnect パッケージがプリロードされているリモート HTTP または HTTPS サーバの URL を指定する必要があります。

（注） FDM API 手順を使用して AnyConnect パッケージをアップロードすることもできます。

Security Cloud Control リポジトリから *AnyConnect* パッケージをアップロードする

リモートアクセス VPN 構成ウィザードには、オペレーティングシステムごとの AnyConnect パッケージが Security Cloud Control リポジトリから表示されるため、パッケージを選択してデバイスにアップロードできます。デバイスがインターネットにアクセスでき、DNS が適切に設定されていることを確認してください。

（注） 目的のパッケージが表示されたリストにない場合、またはデバイスがインターネットにアクセスできない場合は、AnyConnect パッケージがプリロードされているサーバーを使用してパッケージをアップロードできます。

手順

ステップ 1 オペレーティングシステムに対応するフィールドをクリックし、AnyConnect パッケージを選択します。

ステップ 2 をクリックして、パッケージをアップロードします。チェックサムが一致しない場合、AnyConnect パッケージのアップロードは失敗します。失敗の詳細については、デバイスの [ワークフロー（workflow）] タブで確認できます。

はじめる前に

必要なオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」をダウンロードしていることを確認してください。最新の機能、バグ修正、セキュリティパッチを確保するには、常に最新の AnyConnect バージョンをダウンロードする必要があります。デバイスのパッケージは定期的に更新してください。

（注） オペレーティングシステム（OS）（Windows、Mac、Linux）ごとに 1 つの AnyConnect をアップロードできます。1 つの OS タイプに対して複数のバージョンをアップロードすることはできません。

手順

ステップ 1 https://software.cisco.com/download/home/283000185 から AnyConnect パッケージをダウンロードします。

- EULA に同意し、K9（暗号化されたイメージ）の権限を持っていることを確認してください。
- 使用しているオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」を選択します。パッケージ名は「anyconnect-win-4.7.04056-webdeploy-k9.pkg」のようになります。Windows、macOS、Linux それぞれに向けたヘッドエンドパッケージがあります。

ステップ 2 AnyConnect パッケージをリモート HTTP または HTTPS サーバーにアップロードします。FDM-managed デバイスから HTTP または HTTPS サーバーへのネットワークルートがあることを確認します。

（注）
AnyConnect パッケージを HTTPS サーバーにアップロードする場合は、以下の手順を実行してください。

- サーバーの信頼できる CA 証明書を Firewall Device Manager から FDM-managed デバイスにアップロードします。証明書のアップロードについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version X.Y』の「Certificates」の章にある「Uploading Trusted CA Certificates」セクションを参照してください。
- 信頼できる CA 証明書を HTTPS サーバーにインストールします。

ステップ 3 リモートサーバーの URL は、認証を求めない直接リンクである必要があります。URL が事前認証されている場合は、RA VPN ウィザードの URL を指定してファイルをダウンロードできます。

ステップ 4 リモートサーバーの IP アドレスが NAT 処理されている場合は、リモートサーバーのロケーションの NAT 処理済みパブリック IP アドレスを指定する必要があります。

新規 *AnyConnect* パッケージのアップロード

次の手順を使用して、バージョン 6.5.0 を実行している FDM-managed デバイスに新しい AnyConnect パッケージをアップロードします。

手順

ステップ 1 手順 1 ～ 4 で、RA VPN 設定を作成します。

ステップ 2 [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] で、Windows、Mac、Linux のエンドポイントに対して別々のパッケージをアップロードできます。

ステップ 3 対応するプラットフォームフィールドで、Windows、Mac、および Linux と互換性のある AnyConnect パッケージが事前にアップロードされているサーバーのパスを指定します。サーバーパスの例：
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.

ステップ 4 をクリックして、パッケージをアップロードします。Security Cloud Control は、パスが到達可能であり、指定されたファイル名が有効なパッケージであるか検証します。検証が成功すると、AnyConnect パッケージの名前が表示されます。RA VPN 設定に FDM-managed デバイスを追加して、AnyConnect パッケージを追加したデバイスにアップロードできます。

ステップ 5 [OK] をクリックします。AnyConnect パッケージが RA VPN 設定に追加されます。

ステップ 6 ここから「RA VPN 設定の作成」の手順の実行に進みます。

次のタスク

VPN 接続を完了するには、ユーザーは AnyConnect クライアントソフトウェアをワークステーションにインストールする必要があります。詳細については、「ユーザーが FTD に AnyConnect クライアントソフトウェアをインストールする方法」を参照してください。

既存の *AnyConnect* パッケージの置換

AnyConnect パッケージがデバイスにすでに存在している場合、これらは RA VPN ウィザードに表示されます。オペレーティングシステムで利用可能なすべての AnyConnect パッケージが、ドロップダウンリストに表示されます。既存のパッケージをリストから選択して、新しいパッケージと置き換えることができます。ただし、新しいパッケージをリストに追加することはできません。

（注） 既存のパッケージを新しいパッケージに置き換える場合は、新しい AnyConnect パッケージが、FDM-managed デバイスが到達できるネットワーク上のサーバーにすでにアップロードされていることを確認してください。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM** をクリックします。

ステップ 3 変更する RA VPN 設定を選択し、[アクション（Actions）] で [編集（Edit）] をクリックします。

ステップ 4 [検出された AnyConnect パッケージ（AnyConnect Packages Detected）] で、既存の AnyConnect パッケージの横に表示される アイコンをクリックします。オペレーティングシステムに複数のバージョンの AnyConnect パッケージがある場合は、置き換えるパッケージをリストから選択して [編集（Edit）] をクリックします。既存のパッケージが対応するフィールドから消去されます。

ステップ 5 新しい AnyConnect パッケージがプリロードされているサーバーのパスを指定し、 をクリックしてパッケージをアップロードします。

ステップ 6 [OK] をクリックします。新しい AnyConnect パッケージが RA VPN 設定に追加されます。

ステップ 7 ステップ 6 から、「RA VPN 設定の作成」に進みます。

AnyConnect パッケージの削除

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM** をクリックします。

ステップ 3 変更する RA VPN 設定を選択し、[アクション（Actions）] で [編集（Edit）] をクリックします。

ステップ 4 [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] で、削除する AnyConnect パッケージの横に表示される アイコンをクリックします。オペレーティングシステムに複数のバージョンの AnyConnect パッケージがある場合は、リストから削除するパッケージを選択します。既存のパッケージが対応するフィールドから消去されます。

（注）
[キャンセル（Cancel）] をクリックすると削除操作が停止し、既存のパッケージが保持されます。

ステップ 5 [OK] をクリックします。 デバイスの [設定ステータス（Configuration Status）] は [未同期（Not Synced）] となります。

（注）
この段階で削除アクションを取り消す場合は、**Security Devices** ページに移動し、[変更の破棄（Discard Changes）] をクリックして、既存の AnyConnect パッケージを保持します。

ステップ 6 設定の変更を確認して、デバイスに展開します。

FDM-Managed デバイスのアイデンティティソースの設定

Microsoft AD レルムや RADIUS サーバーなどのアイデンティティソースは、組織内のユーザーのユーザーアカウントを定義する AAA サーバーおよびデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、Security Cloud Control へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

Objects をクリックしたあと  をクリックし、**[> RA VPNオブジェクト（ASA & FTD）（> RA VPN Objects（ASA & FTD））] > [IDソース（Identity Source）]**を選択してソースを作成します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。適切なフィルタを適用して既存のソースを検索し、それらを管理できます。

Active Directory レルム

Active Directory は、ユーザーアカウントおよび認証情報を提供します。AD レルムを含む設定を FDM-managed デバイスに展開すると、Security Cloud Control は AD サーバーからユーザーとグループを取得します。

このソースは、以下の目的で使用できます。

- リモートアクセス VPN（プライマリ アイデンティティ ソースとして）。AD は RADIUS サーバーと組み合わせて使用可能。
- アイデンティティポリシー（アクティブ認証用、およびパッシブ認証で使用されるユーザー アイデンティティ ソースとして）。
- ユーザーのアクティブ認証に向けたアイデンティティルール。

ユーザーアイデンティティを使用してアクセスコントロールルールを作成可能。詳細は、「アイデンティティポリシーの導入方法」を参照してください。

Security Cloud Control は、24 時間ごとに最新のユーザーグループのリストを要求します。1 つのルールに最大 50 のユーザーまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザーを選択するより有意義です。たとえば、エンジニアリング グループに開発ネットワークへのアクセスを許可するルールを作成し、それに続くルールとして、そのネットワークへの他のすべてのアクセスを拒否するルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバーのエンジニアリング グループに追加するだけです。

Security Cloud Control の Active Directory レルム

AD アイデンティティ オブジェクトを作成するときに、AD レルムを構成します。アイデンティティ ソース オブジェクト ウィザードは、AD サーバーへの接続方法と、AD サーバーがネットワーク内のどこに配置されているかを判断するために役立ちます。

（注） Security Cloud Control で AD レルムを作成すると、アフィリエイト アイデンティティ ソース オブジェクトを作成するとき、およびそれらのオブジェクトをアイデンティティルールに追加するときに、Security Cloud Control は AD パスワードを記憶します。

FDM の Active Directory レルム

Security Cloud Control オブジェクトウィザードから、FDM で作成された AD レルムオブジェクトを指定できます。Security Cloud Control は、FDM で作成された AD レルムオブジェクトの AD パスワードを**読み取らない**ことに注意してください。Security Cloud Control に正しい AD パスワードを手動で入力する必要があります。

Firewall Device Manager で AD レルムを設定するには、デバイスが実行しているバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』で、「Reusable Objects」の章の「**Configuring AD Identity Realms**」を参照してください。

サポートされるディレクトリ サーバー

Windows サーバー 2008 および 2012 で AD を使用できます。

サーバーの設定に関して次の点に注意してください。

- ユーザー グループまたはグループ内のユーザーに対してユーザー制御を実行する場合、ディレクトリ サーバーでユーザー グループを設定する必要があります。サーバーが基本的なオブジェクト階層でユーザーを整理している場合、システムはユーザーグループ制御を実行できません。
- ディレクトリサーバーは、次の表に示すフィールド名を使用して、システムがそのフィールドのサーバーからユーザーメタデータを取得できるようにする必要があります。

メタデータ（Metadata）	Active Directory フィールド
LDAP ユーザ名	samaccountname
名（First name）	givename
Last Name	sn
電子メール アドレス	mail userprincipalname（mail に値が設定されていない場合）
department	department distinguishedname（department に値が設定されていない場合）
電話番号	telephonenumber

ディレクトリ ベースの *DN* の決定

ディレクトリの各プロパティを設定する際、ユーザおよびグループに共通のベース識別名（DN）を指定する必要があります。ベースはディレクトリサーバー内で定義され、ネットワークごとに異なります。アイデンティティ ポリシーが正しく機能するには、適切なベースを入力する必要があります。ベースが誤っていると、ユーザー名またはグループ名が特定されず、アイデンティティに基づくポリシーが機能しなくなります。

（注） 正しいベースを取得するには、ディレクトリ サーバーを担当する管理者に確認してください。

Active Directory の場合、ドメイン管理者として AD サーバにログインし、コマンドプロンプトで **dsquery** のコマンドを次のように使用することで、正しいベースを判別できます。

ユーザ検索ベース

dsquery user コマンドを入力し、ベース識別名を調べたい既知のユーザー名（一部または全体）を指定します。たとえば、次のコマンドでは、「John*」という部分名を使用して、「John」から始まるすべてのユーザーの情報を返します。

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

ベース DN は「DC=csc-lab,DC=example,DC=com」となります。

グループ検索ベース

既知のグループ名を使用して、**dsquery group** コマンドを入力し、ベース DN を判断します。たとえば次のコマンドでは、グループ名「Employees」を使用して識別名を返します。

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

グループのベース DN は、「DC=csc-lab,DC=example,DC=com」となります。

ADSI Edit プログラムを使用して、AD 構造を参照することもできます（**[スタート]**>**[ファイル名を指定して実行]**>**[adsiedit.msc]**）。ADSI Edit で、組織単位（OU）、グループ、ユーザーなど任意のオブジェクトを右クリックし、[プロパティ（Properties）] を選択すると、識別名が表示されます。DC 値の文字列をベースとしてコピーできます。

ベースが正しいことを確認するには、次のように操作します。

手順

ステップ 1 ディレクトリ プロパティの [テスト接続（Test Connection）] ボタンをクリックし、接続を確認します。問題を解決し、ディレクトリ プロパティを保存します。

ステップ 2 変更をデバイスに適用します。

ステップ 3 アクセス ルールを作成して、[ユーザー（Users）] タブを選択し、ディレクトリから既知のユーザーおよびグループ名の追加を試みます。ディレクトリを含むレルム内の一致ユーザー名およびグループ名を入力すると、入力中にオートコンプリートによる候補が表示されます。これらの候補がドロップダウン リストに表示された場合、システムがディレクトリを正常にクエリーできたことが分かります。候補が表示されず、入力した文字列は確実にユーザー名またはグループ名に含まれることが既知である場合には、対応する検索ベースを修正する必要があります。

次のタスク

詳細は「Firepower Threat Defense Active Directory レルムオブジェクトの作成と編集」を参照してください。

RADIUS サーバおよびグループ

RADIUS サーバーを使用して、管理ユーザーを認証および認可できます。

RADIUS サーバーを使用するように機能を設定する場合は、個別のサーバーではなく RADIUS グループを選択します。RADIUS グループは、相互にコピーである RADIUS サーバーの集合です。グループに複数のサーバーがある場合は、それらは、1 つのサーバーが使用できなくなった場合に冗長性を提供する一連のバックアップ サーバーを形成します。ただし、サーバーが 1 つしかない場合でも、機能の RADIUS サポートを設定するには、メンバーが 1 つのグループを作成する必要があります。

このソースは、以下の目的で使用できます。

- 認証、および許可、アカウンティングのアイデンティティソースとしてのリモートアクセス VPN。AD は RADIUS サーバーと組み合わせて使用できます。
- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザー アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

詳細については、「Firepower Threat Defense RADIUS サーバーオブジェクトまたはグループの作成と編集」を参照してください。

関連情報：

- アクティブ ディレクトリ レルム オブジェクトの作成
- RADIUS サーバーオブジェクトまたはグループの作成
- アイデンティティポリシーの設定

アクティブ ディレクトリ レルム オブジェクトの作成または編集

Active Directory レルムオブジェクトについて

AD レルムオブジェクトなどの ID ソースオブジェクトを作成または編集すると、Security Cloud Control は SDC を介して FDM-managed デバイスに設定要求を送信します。次に FDM-managed デバイスは、設定された AD レルムと通信します。

Security Cloud Control は、Firewall Device Manager コンソールを介して設定された AD レルムのディレクトリパスワードを読み取らないことに注意してください。元々 Firewall Device Manager で作成された AD レルムオブジェクトを使用する場合は、ディレクトリパスワードを手動で入力する必要があります。

FTD アクティブ ディレクトリ レルム オブジェクトの作成

次の手順を使用して、オブジェクトを作成します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Objects** をクリックします。

ステップ 3  をクリックしてから、**[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）]** > **[アイデンティティソース（Identity Source）]**をクリックします。

ステップ 4 オブジェクトの [オブジェクト名（Object Name）] を入力します。

ステップ 5 [デバイスタイプ（Device Type）] として [FTD] を選択します。

ステップ 6 ウィザードの最初の部分で、[IDソースタイプ（Identity Source Type）]として [Active Directory レルム（Active Directory Realm）] を選択します。[続行（Continue）] をクリックします。

ステップ 7 基本レルムのプロパティを設定します。

- [ディレクトリユーザー名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザー情報に対して適切な権限を持つユーザーの識別用ユーザー名とパスワード。AD では、昇格されたユーザー特権は必要ありません。ドメイン内の任意のユーザーを指定できます。ユーザー名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

  （注）
  この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザーは、共通名の「users」フォルダの下で設定する必要があります。

- [ベース識別名（Base Distinguished Name）]：ユーザーおよびグループ情報、つまり、ユーザーとグループの共通の親を検索またはクエリするためのディレクトリツリー。例、cn=users,dc=example,dc=com。

- [ADプライマリドメイン（AD Primary Domain）]：デバイスが参加する必要がある完全修飾 AD ドメイン名。例、example.com。

ステップ 8 ディレクトリ サーバのプロパティを設定します。

- [ホスト名またはIPアドレス（Hostname/IP Address）]：ディレクトリサーバーのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。

- [ポート（Port）]：サーバーとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。

- [暗号化（Encryption）]：ユーザーおよびグループの情報のダウンロードに暗号化された接続を使用するには、希望の方法（[STARTTLS] または [LDAPS]）を選択します。デフォルトでは [なし（None）] になっており、ユーザおよびグループの情報がクリア テキストでダウンロードされます。

- [STARTTLS] では、暗号化方式をネゴシエートし、ディレクトリサーバーでサポートされる最も強力な方式を使用します。ポート 389 を使用します。このオプションは、リモート アクセス VPN にレルムを使用する場合はサポートされません。
- [LDAPS] では、LDAP over SSL が必要です。ポート 636 を使用します。

- [信頼できるCA証明書（Trusted CA Certificate）]：暗号化方式を選択する場合、認証局（CA）の証明書をアップロードして、システムとディレクトリサーバーの間で信頼できる接続を有効化します。認証に証明書を使用する場合、証明書のサーバー名は、サーバーの [ホスト名/IPアドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

ステップ 9 （オプション）[テスト（Test）] ボタンを使用して、構成を検証します。

ステップ 10 （オプション）[別の構成を追加（Add another configuration）] をクリックして、複数の AD サーバーを AD レルムに追加します。AD サーバーは互いの複製である必要があり、同じ AD ドメインをサポートする必要があります。したがって、ディレクトリ名、ディレクトリパスワード、ベース識別名などの基本的なレルムプロパティは、その AD レルムに関連付けられたすべての AD サーバーで同じである必要があります。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

FTD アクティブ ディレクトリ レルム オブジェクトの編集

アイデンティティ ソース オブジェクトの編集時にアイデンティティ ソース タイプを変更できないことに注意してください。正しいタイプの新しいオブジェクトを作成する必要があります。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Objects** をクリックします。

ステップ 3 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 4 編集するオブジェクトを選択します。

ステップ 5 詳細パネルの [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 6 ダイアログボックスの値を、上記の手順で作成したときと同じ方法で編集します。下に表示される設定バーを展開し、ホスト名/IP アドレスや暗号化情報を編集またはテストします。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Security Cloud Control は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ステップ 9 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

RADIUS サーバーオブジェクトまたはグループの作成または編集

RADIUS サーバーオブジェクトまたはグループについて

RADIUS サーバーオブジェクトや RADIUS サーバーオブジェクトのグループなどの ID ソースオブジェクトを作成または編集すると、Security Cloud Control は SDC を介して設定要求を FDM-managed デバイスに送信します。次に FDM-managed デバイスは、設定された AD レルムと通信します。

RADIUS サーバーオブジェクトの作成

RADIUS サーバーは、AAA（認証、認可、アカウンティング）サービスを提供します。

次の手順を使用して、オブジェクトを作成します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Objects** をクリックします。

ステップ 3 をクリックしてから、**[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）]** > **[アイデンティティソース（Identity Source）]**をクリックします。

ステップ 4 オブジェクトの [オブジェクト名（Object name）] を入力します。

ステップ 5 [デバイスタイプ（Device Type）] として [FTD] を選択します。

ステップ 6 [アイデンティティソース（Identity Source）] タイプとして [RADIUSサーバー（RADIUS Server）] を選択します。[続行（Continue）] をクリックします。

ステップ 7 次のプロパティを使用して ID ソース設定を編集します。

- [サーバー名または IP アドレス（Server Name or IP Address）]：サーバーの完全修飾ホスト名（FQDN）または IP アドレス。
- [認証ポート（Authentication Port）]（オプション）：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [タイムアウト（Timeout）]：次のサーバーに要求を送信する前にサーバーからの応答を待機する時間の長さ（1 ～ 300 秒）。デフォルトは 10 秒です。
- [サーバー秘密キー（Server Secret Key）] の入力（オプション）：Firepower Threat Defense デバイスと RADIUS サーバー間でデータを暗号化するために使用される共有秘密。キーは、大文字と小文字が区別される最大 64 文字の英数字文字列です。スペースは使用できません。キーは、英数字または下線で開始する必要があります。特殊文字 $ & - _ . + @ を使用できます。文字列は、RADIUS サーバーで設定された文字列と一致している必要があります。秘密キーを設定していない場合、接続は暗号化されません。

ステップ 8 ネットワークで Cisco Identity Services Engine（ISE）をすでに設定してて、リモートアクセス VPN の認可変更設定のためにサーバーを使用している場合は、[RA VPNのみ（RA VPN Only）] リンクをクリックし、次の項目を設定します。

- [ACLのリダイレクト（Redirect ACL）]：RA VPN リダイレクト ACL を使用する拡張アクセス制御リスト（ACL）を選択します。拡張 ACL がない場合は、FDM-managed デバイスコンソールの Smart CLI テンプレートから必要な拡張 ACL オブジェクトを作成する必要があります。デバイスが実行しているバージョンについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Advanced Configuration」の章の「**Configuring Smart CLI Objects**」セクションを参照してください。リダイレクト ACL の目的は、クライアントポスチャを評価するために、初期トラフィックを ISE に送信することです。ACL は、ISE に HTTPS トラフィックを送信しますが、ISE 宛てのトラフィックや、名前解決のために DNS サーバーに送信されるトラフィックは送信しません。デバイスが実行しているバージョンについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Virtual Private Networks (VPN)」の章の「**Configure Change of Authorization**」セクションを参照してください。
- [診断インターフェース（Diagnostic Interface）]：このオプションを有効にすると、システムは常に「診断」インターフェースを使用してサーバーと通信できるようになります。このオプションを無効のままにすると、Security Cloud Control はデフォルトでルーティングテーブルを使用して、使用するインターフェイスを決定します。

ステップ 9 [追加（Add）] をクリックします。

ステップ 10 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

RADIUS サーバーグループの作成

RADIUS サーバーグループには、1 つまたは複数の RADIUS サーバーオブジェクトが含まれています。グループ内のサーバーは、相互にコピーされる必要があります。グループ内のサーバーでバックアップサーバーのチェーンが形成されるため、最初のサーバーが利用できなった場合、システムはリスト上の次のサーバーを試すことができます。

次の手順を使用して、オブジェクトグループを作成します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Objects** をクリックします。

ステップ 3  をクリックしてから、**[FTD]** > **[アイデンティティソース（Identity Source）]**をクリックします。

ステップ 4 オブジェクトの [オブジェクト名（Object name）] を入力します。

ステップ 5 [デバイスタイプ（Device Type）] として [FTD] を選択します。

ステップ 6 [IDソースタイプ（Identity Source Type）] として [RADIUSサーバーグループ（RADIUS Server Group）] を選択します。[続行（Continue）] をクリックします。

ステップ 7 次のプロパティを使用して ID ソース設定を編集します。

- [デッドタイム（Dead Time）]：失敗したサーバーは、すべてのサーバーが失敗した後にのみ再アクティブ化されます。デッドタイムは、最後のサーバーが失敗した後にすべてのサーバーを再アクティブ化するまで待機する時間の長さです。
- [最大失敗試行回数（Maximum Failed Attempts）]：次のサーバーを試行する前に、グループ内の RADIUS サーバーに送信されて失敗した要求の数（応答がなかった要求の数）。最大失敗試行回数を超えると、システムはそのサーバーを故障としてマークします。特定の機能について、ローカルデータベースを使用するフォールバック方式を設定していて、グループ内のすべてのサーバーが応答に失敗した場合、そのグループは非応答と見なされ、フォールバック方式が試行されます。サーバー グループはデッド タイムの間、非応答とマークされたままになるため、その期間内に追加の AAA 要求でサーバー グループへの接続は試行されず、フォールバック方式がすぐに使用されます。
- （任意）[ダイナミック認証/ポート（Dynamic Authorization/Port）]：RADIUS サーバーグループ向けの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にすると、そのグループは CoA 通知用に登録され、Cisco Identity Services Engine（ISE）からの CoA ポリシー更新を指定したポートでリッスンします。このサーバー グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ動的認可をイネーブルにします。

ステップ 8 ドロップダウンメニューから、RADIUS サーバーをサポートする AD レルムを選択します。AD レルムをまだ作成していない場合は、ドロップダウンメニューの [作成（Create）] をクリックします。

ステップ 9 [追加（Add）] ボタン  をクリックして、既存の RADIUS サーバーオブジェクトを追加します。必要に応じて、このウィンドウから新しい RADIUS サーバーオブジェクトを作成できます。

（注）
リストの最初のサーバーは応答しなくなるまで使用されるため、作成したサーバーオブジェクトを優先して追加します。その後、FDM-managedデバイスはデフォルトでリスト内の次のサーバーに設定されます。

ステップ 10 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

RADIUS サーバーオブジェクトまたはグループの編集

RADIUS サーバーオブジェクトまたは RADIUS サーバーグループを編集するには、次の手順を使用します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Objects** をクリックします。

ステップ 3 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 4 編集するオブジェクトを選択します。

ステップ 5 詳細パネルの [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 6 前述の手順で作成したのと同じ方法で、ダイアログボックスの値を編集します。ホスト名/IP アドレスまたは暗号化情報を編集またはテストするには、設定バーを展開します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Security Cloud Control は、変更の影響を受けるポリシーを表示します。[確認（Confirm）] をクリックして、オブジェクトとその影響を受けるポリシーへの変更を確定します。

ステップ 9 行った変更を今すぐレビューして展開するか、待機してから複数の変更を同時に展開します。

新しい RA VPN グループポリシーの作成

グループポリシーは、リモートアクセス VPN ユーザーの一連のユーザー指向属性値ペアです。接続プロファイルでは、トンネル確立後、ユーザー接続の条件を設定するグループ ポリシーが使用されます。グループ ポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

システムには、「DfltGrpPolicy」という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

（注） 不整合のあるグループ ポリシー オブジェクトを RA VPN 設定に追加することはできません。グループポリシーを RA VPN 設定に追加する前に、すべての不整合を解決してください。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Objects** をクリックします。

ステップ 3 > **[RA VPNオブジェクト（Cisco ASAおよびFTD）（RA VPN Objects (ASA & FTD)）]** > **[RA VPNグループポリシー（RA VPN Group Policy）]** の順にクリックします。

ステップ 4 グループ ポリシーの名前を入力します。名前には最大 64 文字の長さを使用でき、スペースも使用できます。

ステップ 5 [デバイスタイプ] ドロップダウンで、[FTD] を選択します。

ステップ 6 次のいずれかを実行します。

- 必要なタブをクリックし、そのページで属性を設定します。
  - 一般属性
  - AnyConnect クライアント プロファイル （105 ページ）
  - セッション設定属性 （106 ページ）
  - アドレス割り当て属性 （107 ページ）
  - スプリット トンネリング属性 （107 ページ）
  - AnyConnect 属性 （108 ページ）
  - トラフィック フィルタ属性 （110 ページ）
  - Windows ブラウザ プロキシ属性 （111 ページ）

ステップ 7 [保存（Save）] をクリックしてグループポリシーを作成します。

RA VPN グループポリシー属性

グループポリシーの全般的な属性では、グループの名前およびその他の基本設定を定義します。名前属性は唯一の必須属性です。

- [DNSサーバー（DNS Server）]：VPN に接続する際、クライアントがドメイン名の解決に使用する DNS サーバークライアントを定義する DNS サーバーグループを選択します。必要なグループがまだ定義されていない場合は、[DNSグループの作成（Create DNS Group）] をクリックしてすぐに作成します。
- **Banner**：ユーザーのログイン時に表示するバナーテキストまたはウェルカムメッセージです。デフォルトでは、バナーは表示されません。最大文字数は496 文字です。AnyConnect クライアントは、部分的な HTML をサポートしています。リモート ユーザーへバナーが適切に表示されることを確認するには、
 タグを使用して改行を示します。
- [デフォルトドメイン（Default Domain）]：RA VPN 内のユーザーのデフォルトドメインの名前。例、example.com。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。
- [AnyConnectクライアントプロファイル（AnyConnect Client Profiles）]：[+] をクリックし、このグループに使用する AnyConnectクライアントプロファイルを選択します。「AnyConnect クライアントプロファイルの設定とアップロード」を参照してください。外部インターフェイスの完全修飾ドメイン名を設定すると（接続プロファイルで）、デフォルトプロファイルが自動的に作成されます。代わりに、自分用のクライアントプロファイルをアップロードすることもできます。スタンドアロン AnyConnect プロファイルエディタを使用してこれらのプロファイルを作成します。スタンドアロンAnyConnectプロファイルエディタは、software.cisco.com からダウンロードしてインストールできます。クライアントプロファイルを選択しない場合、AnyConnect クライアントはすべてのオプションにデフォル

ト値を使用します。このリストの項目は、プロファイル自体ではなく AnyConnect クライアント プロファイル オブジェクトです。新しいプロファイルを作成（およびアップロード）するには、ドロップダウンリストで [新規 AnyConnectクライアントプロファイルの作成（Create New AnyConnect Client Profile）] をクリックします。

AnyConnect クライアント プロファイル

この機能は、ソフトウェアバージョン 6.7 以降のバージョンを実行している Firewall Device Manager でサポートされています。

Cisco AnyConnect VPN クライアントは、さまざまな組み込みモジュールによって、強化されたセキュリティを提供します。これらのモジュールは、Web セキュリティ、エンドポイントフローに対するネットワークの可視性、オフネットワークローミング保護などのサービスを提供します。各クライアントモジュールには、要件に応じたカスタム設定のグループを含むクライアントプロファイルが含まれています。

VPN ユーザーが VPN AnyConnect クライアントソフトウェアをダウンロードするときに、クライアントにダウンロードする AnyConnect VPN プロファイルオブジェクトと AnyConnect モジュールを選択できます。

1. AnyConnect VPN プロファイルオブジェクトを選択または作成します。「RA VPN AnyConnect クライアントプロファイルのアップロード （126 ページ）」を参照してください。DART および Start Before Login モジュールを除き、AnyConnect VPN プロファイルオブジェクトを選択する必要があります。

2. [AnyConnectクライアントモジュールの追加（Add Any Connect Client Module）] をクリックします。

   次の AnyConnect モジュールはオプションであり、VPN AnyConnect クライアントソフトウェアとともに各モジュールがダウンロードされるように設定できます。

   - **AMP イネーブラ**：エンドポイント向けの高度なマルウェア防御（AMP）を導入します。
   - **DART**：システムログのスナップショットおよびその他の診断情報がキャプチャされて、.zip ファイルがデスクトップに作成されるため、トラブルシューティング情報を簡単に Cisco TAC に送信できます。
   - **フィードバック**：お客様が有効にして使用している機能とモジュールに関する情報を提供します。
   - **ISE ポスチャ**：OPSWAT ライブラリを使用してポスチャチェックを実行し、エンドポイントの適合性を評価します。
   - **Network Access Manager**：有線とワイヤレスの両方のネットワークにアクセスするための 802.1X（レイヤ 2）とデバイス認証を備えています。
   - **Network Visibility**：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。

- **Start Before Login**：Windows のログインダイアログボックスが表示される前に AnyConnect を開始することにより、Windows にログインする前のユーザーを VPN 接続を介して企業インフラストラクチャに強制的に接続させます。
- **Cisco Umbrella Roaming Security**：アクティブな VPN がないときに DNS レイヤセキュリティを提供します。
- **Web セキュリティ**：定義されているセキュリティポリシーに基づいて、Web ページの要素を分析し、許容可能なコンテンツを許可し、悪意のあるコンテンツまたは許容できないコンテンツをブロックします。

3. [クライアントモジュール（Client Module）] リストで [AnyConnect] モジュールを選択します。
4. [プロファイル（Profile）] リストで、AnyConnect クライアントプロファイルを含むプロファイルオブジェクトを選択または作成します。
5. [モジュールのダウンロードを有効化（Enable Module Download）] をオンにすると、エンドポイントでプロファイルとともにクライアントモジュールをダウンロードできます。オフの場合、エンドポイントはクライアントプロファイルだけをダウンロードできます。

セッション設定属性

グループポリシーのセッションの設定は、VPN を通じて接続できる時間と、接続を確立できる個別の接続数を制御します。

- [最大接続時間（Maximum Connection Time）]：ユーザーがログアウト、再接続せずに VPN に接続したままにできる最大時間（分）で、1 ～ 4473924 または空白で指定します。デフォルトは無制限（空白）ですが、その場合でもアイドル タイムアウトは適用されます。
- [接続時間のアラート間隔（Connection Time Alert Interval）]：最大接続時間を指定した場合、アラート間隔は、次回の自動切断についてユーザーに警告を表示する最大時間に達するまでの時間を定義します。ユーザーは、接続を終了し、再接続してタイマーを再起動することを選択できます。デフォルトは 1 分です。1 ～ 30 分を指定できます。
- [アイドルタイム（Idle Time）]：VPN 接続が自動的に閉じられる前にアイドル状態になる時間（分）で、1 ～ 35791394 で指定します。指定した時間、接続で通信アクティビティがない場合、システムは接続を停止します。デフォルトは 30 分です。
- [アイドル時間のアラート間隔（Idle Time Alert Interval）]：アイドルセッションが原因の次回の自動切断について、ユーザーに警告を表示するアイドル時間に達するまでの時間。アクティビティがあるとタイマーがリセットされます。デフォルトは 1 分です。1 ～ 30 分を指定できます。
- [ユーザーあたりの同時ログイン数（Simultaneous Login Per User）]：ユーザーに許可する同時接続の最大数。デフォルトは 3 です。1 ～ 2147483647 個の接続を指定できます。多数の同時接続を許可するとセキュリティの低下を招き、パフォーマンスに影響を及ぼす可能性があります。

アドレス割り当て属性

グループポリシーのアドレスの割り当て属性は、グループのIPアドレスプールを定義します。ここで定義されているプールで、このグループを使用するすべての接続プロファイルで定義済みのプールがオーバーライドされます。接続プロファイルで定義済みのプールを使用する場合は、これらの設定を空白のままにします。

- [IPv4アドレスプール（IPv4 Address Pool）]、[IPv6アドレスプール（IPv6 Address Pool）]：これらのオプションは、リモートエンドポイントのアドレスプールを定義します。クライアントには、VPN 接続のために使用する IP バージョンに基づき、これらのプールからアドレスが割り当てられます。サポートする IP タイプごとにサブネットを定義するネットワーク オブジェクトを選択します。当該 IP バージョンをサポートしない場合は、リストを空のままにします。たとえば、IPv4 プールを「10.100.10.0/24」と定義できます。アドレス プールは、外部インターフェイスの IP アドレスと同じサブネット上に存在することはできません。ローカルアドレスの割り当てに使用する最大6個のアドレスプールのリストを指定できます。プールの指定順序は重要です。システムでは、プールの表示順に従いプールからアドレスが割り当てられます。

- [DHCPスコープ（DHCP Scope）]：接続プロファイルのアドレスプールに DHCP サーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じプール内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用する DHCP サーバーで定義されているアドレスプールのサブセットを選択できます。ネットワーク スコープを定義しない場合、DHCP サーバーはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。スコープを指定するには、ネットワーク番号のホストアドレスを含むネットワークオブジェクトを選択します。オブジェクトがまだ存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックします。たとえば、192.168.5.0/24 サブネットプールのアドレスを使用するように DHCP サーバーに指示するには、ホストアドレスとして192.168.5.0を指定するネットワークオブジェクトを選択します。DHCP は IPv4 アドレス指定にのみ使用することができます。

スプリット トンネリング属性

グループポリシーのスプリットトンネリング属性は、システムが内部ネットワーク用のトラフィックと外部方向トラフィックを処理する方法を定義します。スプリットトンネリングは、VPN トンネル（暗号化）と VPN トンネル外の残りのネットワークトラフィック（非暗号化、つまりクリアテキスト）を介して一部のネットワークトラフィックを誘導します。

- [IPv4スプリットトンネリング（IPv4 Split Tunneling）]、[IPv6スプリットトンネリング（IPv6 Split Tunneling）]：トラフィックが IPv4 または IPv6 アドレスを使用するかどうかに基づいて、さまざまなオプションを指定できますが、それぞれのオプションは同じです。スプリットトンネリングを有効にする場合は、ネットワークオブジェクトを選択する必要があるいずれかのオプションを指定します。

  - [トンネル経由のトラフィックをすべて許可する（Allow all traffic over tunnel）]：スプリットトンネリングを行いません。ユーザーがRA VPN接続を行うと、そのユーザー

のトラフィックはすべて保護されたトンネルを通過します。これがデフォルトです。最も安全なオプションであるとも考えられます。

- [トンネル経由で指定されたトラフィックを許可する（Allow specified traffic over the tunnel）]：宛先ネットワークとホストアドレスを定義するネットワークオブジェクトを選択します。これらの宛先へのトラフィックすべては、保護されたトンネルを通過します。その他すべての宛先へのトラフィックは、クライアントによって、トンネル外の接続（ローカル Wi-Fi やネットワーク接続など）にルーティングされます。
- [以下に指定したネットワークを除外する（Exclude networks specified below）]：宛先ネットワークまたはホストアドレスを定義するネットワークオブジェクトを選択します。クライアントは、指定された宛先へのトラフィックをトンネル外の接続にルーティングします。他の宛先へのトラフィックはトンネルを通過します。

- [スプリットDNS（Split DNS）]：クライアントが、そのクライアントで設定されている DNS サーバーに他の DNS 要求を送信することを許可しながら、セキュアな接続を介して一部の DNS 要求を送信するようにシステムを設定できます。次の DNS 動作を設定できます。
  - [スプリットトンネルポリシーに従ってDNS要求を送信する（Send DNS Request as per split tunnel policy）]：このオプションを選択すると、スプリットトンネル オプションが定義されているのと同じ方法で DNS 要求が処理されます。スプリットトンネリングを有効にすると、DNS 要求は宛先アドレスに基づいて送信されます。スプリットトンネリングを有効にしていない場合、DNS 要求はすべて保護された接続を介します。
  - [常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）]：スプリットトンネリングを有効にするが、すべての DNS 要求を保護された接続を介して、グループで定義された DNS サーバーに送信する場合は、このオプションを選択します。
  - [指定したドメインのみをトンネル経由で送信（Send only specified domains over tunnel）]：保護された DNS サーバーが特定のドメインのアドレスだけを解決するようする場合は、このオプションを選択します。次に、ドメインを指定します。ドメイン名はコンマで区切ります。例：example.com, example1.com。内部 DNS サーバーが内部ドメインの名前を解決し、外部 DNS サーバーが他のすべてのインターネットトラフィックを処理するようにする場合は、このオプションを使用します。

AnyConnect 属性

グループポリシーの AnyConnect 属性は、AnyConnect クライアントでリモートアクセス VPN 接続に使用されるいくつかの SSL および接続設定を定義します。

- **SSL 設定**
  - [Datagram Transport Layer Security（DTLS）の有効化（Enable Datagram Transport Layer Security (DTLS)）]：AnyConnect クライアントが SSL トンネルと DTLS トンネルの 2 つのトンネルを同時に使用することを許可するかどうかを指定します。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の

影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。DTLS をイネーブルにしない場合、SSL VPN 接続を確立している AnyConnect クライアント ユーザーは SSL トンネルのみで接続します。

- [DTLS圧縮（DTLS Compression）]：LZS を使用してこのグループの Datagram Transport Layer Security（DTLS）接続を圧縮するかどうかを指定します。[DTLS圧縮（DTLS Compression）] はデフォルトで無効になっています。
- [SSL圧縮（SSL Compression）]：データ圧縮を有効にするかどうかを指定します。有効にする場合、使用するデータ圧縮の方法は（[圧縮（Deflate）] または [LZS]）です。[SSL圧縮（SSL Compression）] はデフォルトで無効になっています。データ圧縮により、伝送速度は上がりますが、各ユーザーセッションのメモリ要件と CPU 使用率も高くなるため、SSL 圧縮はデバイスの全体的なスループットを低下させます。
- [SSLキーの再生成方法（SSL Rekey Method）]、[SSLキーの再生成間隔（SSL Rekey Interval）]：クライアントは、暗号キーと初期化ベクトルを再ネゴシエーションしながら VPN 接続キーを再生成して、接続のセキュリティを強化します。[なし（None）] を選択して、キーの再生成を無効にします。キーの再生成を有効にするには、新しいトンネルを作成するたびに [新しいトンネル（New Tunnel）] を選択します（[既存のトンネル（Existing Tunnel）] オプションは、[新しいトンネル（New Tunnel）] と同じアクションになります）。キーの再生成を有効にする場合は、キーの再生成間隔も設定します。デフォルトは 4 分です。間隔は、4 ～ 10080 分（1 週間）の範囲で設定できます。

• 接続の設定

- [DF（Don't Fragment）ビットを無視する（Ignore the DF (Don't Fragment) bit）]：フラグメント化が必要なパケットの Don't Fragment（DF）ビットを無視するかどうかを指定します。DF ビットが設定されているパケットの強制フラグメンテーションを許可し、それらのパケットがトンネルを通過できるようにするには、このオプションを選択します。
- [クライアントバイパスプロトコル（Client Bypass Protocol）]：セキュアゲートウェイによる（IPv6 トラフィックだけを予期しているときの）IPv4 トラフィックの管理方法や、（IPv4 トラフィックだけを予期しているときの）IPv6 トラフィックの管理方法を設定することができます。

  AnyConnect クライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが AnyConnect 接続に IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合、ヘッドエンドが IP アドレスを割り当てなかったネットワークトラフィックについて、Client Bypass Protocol によってそのトラフィックをドロップさせるか（デフォルト、無効、オフ）、またはヘッドエンドをバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するか（有効、オン）を設定できます。

  たとえば、セキュア ゲートウェイが AnyConnect 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアント バイパ

ス プロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

- [MTU]：Cisco AnyConnect VPN Client によって確立された SSL VPN 接続の最大伝送ユニット（MTU）サイズ。デフォルトは 1406 バイトで、範囲は 576 ー 1462 バイトです。
  - [AnyConnectとVPNゲートウェイ間のキープアライブメッセージ（Keepalive Messages Between AnyConnect and VPN Gateway）]：トンネルでのデータの送受信にピアを使用できることを示すために、ピア間でキープアライブメッセージを交換するかどうかを指定します。キープアライブ メッセージは、設定された間隔で送信されます。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。
  - [ゲートウェイ側の間隔でのDPD（DPD on Gateway Side Interval）]、[クライアント側の間隔でのDPD（DPD on Client Side Interval）]：ピアが応答しなくなったときに VPN ゲートウェイまたは VPN クライアントによる迅速な検出を確実に実行するには、Dead Peer Detection（DPD; デッドピア検出）を有効にします。ゲートウェイまたはクライアント DPD を個別に有効にすることができます。DPD メッセージのデフォルトの送信間隔は 30 秒です。間隔は、5～3600 秒にすることができます。

トラフィック フィルタ属性

グループポリシーのトラフィックフィルタ属性は、グループに割り当てられているユーザーに適用する制限を定義します。アクセス コントロール ポリシー ルールを作成する代わりにこれらの属性を使用することで、ホストまたはサブネットアドレスとプロトコル、または VLAN に基づいて、RA VPN ユーザーのアクセスを特定のリソースに制限できます。デフォルトでは、RA VPN ユーザーは、保護されたネットワーク上の宛先へのアクセスがグループポリシーによって制限されることはありません。

- [アクセスリストフィルタ（Access List Filter）]：拡張アクセス制御リスト（ACL）を使用してアクセスを制限します。Smart CLI 拡張 ACL オブジェクトを選択します。拡張 ACL では、送信元アドレス、宛先アドレス、およびプロトコル（IP や TCP など）に基づいてフィルタリングできます。ACL はトップダウン方式で最初に一致したものから評価されるため、具体的なルールはより一般的なルールの前に配置してください。ACL の末尾には、暗黙的な「deny any」があるため、いくつかのサブネットへのアクセスを拒否しながら、他のすべてのアクセスを許可する場合は、ACL の最後に「permit any」ルールを含めてください。拡張 ACL スマート CLI オブジェクトを編集しながらネットワークオブジェクトを作成することはできないため、グループポリシーを編集する前に、ACL を作成する必要があります。そうしないと、単純にオブジェクトを作成し、後でもう一度ネットワークオブジェクトを作成し、その後で必要なすべてのアクセス制御エントリを作成する必要があります。ACL を作成するには、Firewall Device Manager にログインして、**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（Smart CLI）]** > **[オブジェクト（Objects）]** に移動し、オブジェクトを作成して、オブジェクトタイプとして [拡張アクセスリスト（Extended Access List）] を選択します。

- [VPNをVLANに制限（Restrict Access to VLAN）]：「VLAN マッピング」とも呼ばれるこの属性で、このグループポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。システムは、このグループからのトラフィックすべてを、選択したVLANに転送します。この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。デバイスのサブインターフェイスで定義されている VLAN 番号を指定していることを確認します。値の範囲は 1 ～ 4094 です。

Windows ブラウザ プロキシ属性

グループポリシーの Windows ブラウザプロキシ属性は、ユーザーのブラウザで定義されたプロキシが動作しているかどうか、およびその動作方法を判断します。

[VPNセッション中のブラウザプロキシ（Browser Proxy During VPN Session）] に対して次のいずれかの値を選択できます。

- [エンドポイント設定のまま（No change in endpoint settings）]：HTTP のブラウザプロキシを設定するかどうかをユーザーが決定できます。設定されている場合、そのプロキシが使用されます。
- [ブラウザプロキシの無効化（Disable browser proxy）]：ブラウザに定義されているプロキシ（ある場合）を使用しません。どのブラウザ接続もプロキシを経由しません。
- [自動検出設定（Auto detect settings）]：クライアントデバイスのブラウザでの自動プロキシサーバー検出の使用を有効にします。
- [カスタム設定を使用（Use custom settings）]：HTTP トラフィックに対してすべてのクライアントデバイスで使用する必要があるプロキシを定義します。次を設定します。
  - [プロキシサーバーのIPまたはホスト名（Proxy Server IP or Hostname）]、[ポート（Port）]：プロキシサーバーの IP アドレスまたはホスト名、およびプロキシサーバーが使用するプロキシ接続のポート。ホストとポートを組み合わせた文字数が 100 文字を超えることはできません。
  - [ブラウザプロキシ免除リスト（Browser Proxy Exemption List）]：免除リストにあるホスト/ポートへの接続はプロキシを経由しません。プロキシを使用すべきでない宛先のすべてのホスト/ポート値を追加します。例：www.example.com ポート 80。[プロキシ例外の追加（Add proxy exception）] をクリックしてリストに項目を追加します。項目を削除するには、ごみ箱アイコンをクリックします。すべてのアドレスとポートを合わせたプロキシ例外リスト全体で、255 文字を超えることはできません。

RA VPN 設定の作成

Security Cloud Control を使用すると、1 つ以上の FDM-managed デバイスを RA VPN 構成ウィザードに追加し、デバイスに関連付けられた VPN インターフェイス、アクセス制御、および NAT 免除設定を設定できます。したがって、各 RA VPN 設定には、RA VPN 設定に関連付けられた複数の FDM-managed デバイス間で共有される接続プロファイルとグループポリシーを

含めることができます。さらに、接続プロファイルとグループポリシーを作成して、設定を拡張できます。

RA VPN 設定がすでに設定されている FDM-managed デバイス、または RA VPN 設定がない新しいデバイスを導入準備できます。RA VPN 設定がすでにある FDM-managed デバイスを導入準備すると、Security Cloud Control は自動的に「デフォルトの RA VPN 設定」を作成し、FDM-managed デバイスをこの設定に関連付けます。このデフォルト設定には、デバイスで定義されているすべての接続プロファイルオブジェクトを含めることができます。

重要

- 同じリモートアクセス VPN 設定には、Cisco ASA と FDM-managed デバイスを追加できません。
- FDM-managed デバイスに、1 つ以上の RA VPN 設定は設定できません。

前提条件

FDM-managed デバイスを RA VPN 設定に追加する前に、次の前提条件が満たされている必要があります。

- FDM-managed デバイスに以下が含まれていることを確認します。
  - 有効な ライセンス。詳細については、「リモートアクセス VPN のライセンス要件」を参照してください。
  - FDM バージョン 6.4.0 の場合、少なくとも 1 つの AnyConnect ソフトウェアパッケージがデバイスに事前にアップロードされていることを確認してください。詳細については、「AnyConnect ソフトウェアパッケージの Firepower Threat Defense デバイスバージョン 6.4.0 へのアップロード」を参照してください。
  - FDM バージョン 6.5.0 以降では、Security Cloud Control を使用して AnyConnect パッケージをアップロードできます。詳細については、「AnyConnect ソフトウェアパッケージの Firepower Threat Defense デバイスバージョン 6.5.0 へのアップロード」を参照してください。
  - 保留中の設定展開がない。
- FDM の変更は Security Cloud Control に同期されます。
  1. 左側のペインで、**Security Devices** をクリックし、同期する 1 つ以上の FDM-managed デバイスを検索します。
  2. 1 つ以上のデバイスを選択し、[変更の確認（Check for Changes）] をクリックします。Security Cloud Control は 1 つ以上の FDM-managed デバイスと通信して変更を同期します。
- RA VPN 設定グループポリシーのオブジェクトは一貫しています。

- 一貫性のないすべてのグループポリシーのオブジェクトはRA VPN設定に追加できないため、それらが解決されていることを確認します。問題に対処するか、一貫性のないグループポリシーのオブジェクトを[オブジェクト（Objects）]ページから削除します。詳細については、「重複オブジェクト問題の解決」および「一貫性のないオブジェクト問題の解決」を参照してください。

- FDM-managed デバイスの RA VPN グループポリシーは、RA VPN 設定グループポリシーと一致しています。

手順

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM** をクリックします。

ステップ 3 青色のプラス ボタンをクリックして、新しい RA VPN 設定を作成します。

ステップ 4 リモートアクセス VPN の設定の名前を入力します。

ステップ 5 青色のプラス ボタンをクリックして、FDM-managed デバイスを設定に追加します。デバイスの詳細を追加し、デバイスに関連付けられたネットワークトラフィック関連の権限を設定できます。

1. 次のデバイスの詳細を提供します。

   - [デバイス（Device）]：追加する FDM-managed デバイスを選択し、[選択（Select）] をクリックします。

     重要
     同じリモートアクセス VPN 設定には、Cisco ASA と FDM-managed デバイスを追加できません。

   - [デバイスアイデンティティ証明書（Certificate of Device Identity）]：デバイスのアイデンティティを確立するために使用する内部証明書を選択します。内部証明書は、AnyConnect クライアントがデバイスへの接続を行うときにデバイスのアイデンティティを確立します。安全な VPN 接続を完了するには、クライアントがこの証明書を承認する必要があります。まだ証明書がない場合、ドロップダウンリストの [新規内部証明書の作成（Create New Internal Certificate）] をクリックします。「自己署名内部および内部 CA 証明書の生成」を参照してください。

   - [外部インターフェイス（Outside Interface）]：リモートアクセス VPN 接続を確立するときにユーザーが接続するインターフェイス。これは、通常外部（インターネットに接続された）インターフェイスですが、デバイスとこの接続プロファイルがサポートしているエンドユーザー間のいずれかのインターフェイスを選択します。

新しいサブインターフェイスを作成するには、「Firepower VLAN サブインターフェイスと 802.1Q トランキングの設定」を参照してください。

- [外部インターフェイスの完全修飾ドメイン名またはIP（Fully-qualified Domain Name or IP for the Outside Interface）]：インターフェイスの名前（例、ravpn.example.com）または IP アドレスを指定する必要があります。名前を指定すると、クライアント プロファイルが作成されます。**注**：ユーザーは、クライアントによって VPN で使用される DNS サーバーが、この名前から外部インターフェイスの IP アドレスを解決できるようにする必要があります。関連する DNS サーバーに FQDN を追加します。

2. [続行（Continue）] をクリックして、トラフィックの権限を設定します。

   - [復号されたトラフィック（sysopt permit-vpn）に対するバイパスアクセスコントロールポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：デフォルトでは、復号されたトラフィックは、アクセス コントロール ポリシーの検査の対象になります。このオプション [複合されたトラフィックのバイパス（bypasses the decrypted traffic）] オプションを有効にすると、アクセス コントロール ポリシーの検査がバイパスされますが、AAA サーバーからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。このオプションを選択すると、システムによりグローバル設定である sysopt connection permit-vpn コマンドが設定されることに注意してください。これは、サイト間 VPN 接続の動作にも影響を及ぼします。このオプションを選択しない場合、外部ユーザーがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングし、ネットワークにアクセスするおそれがあります。この理由は、アドレスプールに内部リソースへのアクセスを許可するアクセスコントロールルールを作成する必要があるためです。アクセスコントロールルールを使用する場合は、送信元IPアドレスだけではなく、ユーザーの仕様を使用してアクセスを制御することを検討してください。このオプションを選択することの欠点は、VPN トラフィックが検査されないことです。つまり、侵入およびファイル保護、URL フィルタリング、または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。

   - [NAT免除（NAT Exempt）]：リモートアクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を有効にします。VPN トラフィックを NAT 免除にしない場合は、外部および内部インターフェイスに対する既存の NAT ルールが RA VPN アドレス プールに適用されないことを確認してください。NAT 免除 ルールは特定の送信元/宛先インターフェイスとネットワークの組み合わせに対する手動スタティック アイデンティティ NAT ルールですが、NAT ポリシーには反映されず、非表示になります。NAT 免除を有効にした場合、以下も設定する必要があります。

     - [内部インターフェイス（Inside Interfaces）]：リモートユーザーがアクセスする内部ネットワークのインターフェイスを選択します。これらのインターフェイスには NAT ルールが作成されます。

     - [内部ネットワーク（Inside Networks）]：リモートユーザーがアクセスする内部ネットワークを表すネットワークオブジェクトを選択します。ネットワーク リス

トには、サポートしているアドレス プールと同じ IP タイプを含める必要があります。

ステップ 6 [OK] をクリックします。

- Firewall Device Manager バージョン 6.4.0 デバイスをオンボードしている場合、[検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] には、デバイスで使用可能な AnyConnect パッケージが表示されます。
- Firewall Device Manager バージョン 6.5.0 以降のデバイスをオンボードしている場合は、AnyConnect パッケージが事前にアップロードされているサーバーから AnyConnect パッケージを追加する必要があります。手順については、「FDM 管理対象バージョン 6.5.0 への AnyConnect ソフトウェアパッケージのアップロード」を参照してください。

ステップ 7 [OK] をクリックします。デバイスが設定に追加されます。

次のタスク

（注） 設定を選択し、[アクション（Actions）] で適切なアクションをクリックします。

- [グループポリシー（Group Policies）]：グループポリシーを追加または削除します。
  - [+] をクリックして、必要なグループポリシーを選択します。新しい RA VPN グループポリシーを作成するには、「新しい FTD RA VPN グループポリシーの作成」を参照してください。
- [削除（Remove）]：選択した RA VPN 設定を削除します。

RA VPN 設定の変更

既存の RA VPN 設定の名前とデバイスの詳細を変更できます。

手順

変更する設定を選択し、[アクション（Actions）] の下で [編集（Edit）] をクリックします。

- 必要に応じて名前を変更します。
- 青色のプラス ボタンをクリックして、新しいデバイスを追加します。
- をクリックして、FDM-managed デバイスで次の手順を実行します。

- [編集（Edit）] をクリックして、既存の RA VPN 設定を変更します。
- [削除（Remove）] をクリックして、RA VPN 設定から FDM-managed デバイスを削除します。グループポリシーを除き、そのデバイスに関連付けられているすべての接続プロファイルと RA VPN 設定が削除されます。グループポリシーは、オブジェクトページから明示的に削除できます。**注**：FDM-managed デバイスが設定を使用している唯一のデバイスの場合は削除できません。代わりに、RA VPN 設定を削除できます。

設定またはデバイスの名前を入力して、リモートアクセス VPN 設定を検索することもできます。

関連情報：

- FTD RA VPN 接続プロファイルを設定します。
- 設定の変更を確認して、デバイスに展開します。
- リモートアクセス VPN によるトラフィックを許可します。

RA VPN 接続プロファイルの設定

RA VPN 接続プロファイルの定義する接続特性では、外部ユーザーが AnyConnect クライアントを使用してシステムに VPN 接続することを許可します。各プロファイルは、ユーザーの認証に使用される AAA サーバーと証明書、ユーザーの IP アドレスを割り当てるためのアドレスプール、およびさまざまなユーザー関連の属性を定義するグループポリシーを定義します。

異なるユーザーグループに異なるサービスを提供する必要がある場合、または異なる認証ソースがある場合は、RA VPN 設定内に複数のプロファイルを作成できます。たとえば、自分の組織が異なる認証サーバーを使用する別の組織とマージする場合、別の組織の認証サーバーを使用する新しいグループのプロファイルを作成できます。

RA VPN 接続プロファイルを作成すると、ユーザーは、ホームネットワークなどの外部ネットワークから内部ネットワークに接続できるようになります。異なる認証方式に対応するために、個別のプロファイルを作成します。

はじめる前に

リモート アクセス（RA）VPN 接続を設定する前に、以下のことを行います。

- リモート アクセス VPN 接続を終了する外部インターフェイスは、HTTPS 接続を許可する管理アクセス リストを持つこともできません。RA VPN を設定する前に、外部インターフェイスから HTTPS ルールを削除します。『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド（バージョン X.Y）』内の「システム管理」の章の「管理アクセスリストの構成」を参照してください。
- RA VPN 構成を作成します。『RA VPN 構成の作成』を参照してください。

手順

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM** をクリックします。VPN設定をクリックして、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報を表示できます。

ステップ 3 接続プロファイルをクリックし、右側のサイドバーの [アクション（Actions）] で [接続プロファイルの追加（Add Connection Profile）] をクリックします。

ステップ 4 基本接続の属性を設定します。

- [接続プロファイル名（Connection Profile Name）]：スペースを含めずに最大 50 文字で、この接続の名前を指定します。例、MainOffice。

  （注）
  ここで入力する名前が、AnyConnectクライアントの接続リストに表示されます。ユーザーにとって意味のある名前を選択します。

- [グループエイリアス（Group Alias）]、[グループURL（Group URL）]：エイリアスには特定の接続プロファイルの代替名またはURLが含まれます。VPNユーザーは、FDM-managed デバイスへの接続時に、AnyConnect クライアントの接続リストでエイリアス名を選択できます。接続プロファイル名はグループのエイリアスとして自動的に追加されます。グループ URL のリストも設定できます。このリストは、リモートアクセス VPN 接続を開始するときにエンドポイントが選択できるリストです。ユーザーがグループ URL を使用して接続すると、システムはそのURLに一致する接続プロファイルを自動的に使用します。この URL は、AnyConnect クライアントをまだインストールしていないクライアントによって使用されます。グループエイリアスと URL を必要な数だけ追加します。これらのエイリアスと URL は、デバイスで定義されているすべての接続プロファイルで一意である必要があります。グループ URL は https:// で始まる必要があります。

- たとえば、「Contractor」というエイリアスとグループ URL 「`https://ravpn.example.com/contractor`」があるとします。AnyConnect クライアントをインストールすると、ユーザーは単純に AnyConnect VPN の接続ドロップダウンリストでグループエイリアスを選択します。

ステップ 5 プライマリ アイデンティティ ソース、および必要に応じてセカンダリ ソースを設定します。これらのオプションにより、リモートアクセス VPN 接続を有効にするための、デバイスへのユーザー認証方法が決定されます。最も簡単なアプローチは、AAA のみを使用し、AD レルムを選択するか、または LocalIdentitySource を使用する方法です。[認証タイプ（Authentication Type）] として次のアプローチを使用できます。

- [AAAのみ（AAA Only）]：ユーザー名とパスワードに基づいてユーザーを認証および認可します。詳細については、「接続プロファイルのための AAA の設定」を参照してください。

- [クライアント証明書のみ（Client Certificate Only）]：クライアントデバイスアイデンティティ証明書に基づいてユーザーを認証します。詳細については、「接続プロファイルの証明書認証の設定」を参照してください。
- [AAAおよびクライアント認証（AAA and Client Certificate）]：ユーザー名/パスワードと、クライアントデバイスアイデンティティ証明書の両方を使用します。

ステップ 6 クライアントのアドレスプールを設定します。アドレスプールは、リモートクライアントがVPN 接続を確立するときに、システムがリモートクライアントに割り当てることができる IP アドレスを定義します。詳細については、「クライアントアドレスプール割り当ての設定」を参照してください。

ステップ 7 [続行（Continue）] をクリックします。

ステップ 8 リストからこのプロファイルに対して使用する [グループポリシー（Group Policy）] を選択し、[選択（Select）] をクリックします。グループポリシーは、トンネル確立後のユーザー接続の期間を設定します。システムには、DfltGrpPolicy という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

（注）
必要なグループポリシーがまだ存在しない場合は、[オブジェクト（Objects）]ページでグループポリシーを作成し、そのポリシーをRA VPN設定に関連付けます。グループポリシーの詳細については、「新規 RA VPN グループポリシーの作成」を参照してください。

ステップ 9 [続行（Continue）] をクリックします。

ステップ 10 サマリーを確認します。最初に、サマリーが正しいことを確認します。AnyConnect ソフトウェアをインストールし、VPN接続を完了できることをテストするために、エンドユーザーが最初に行う必要がある内容を確認できます。  をクリックしてこれらの手順をクリップボードにコピーし、ユーザーに配布します。

ステップ 11 [完了（Done）] をクリックします。

次のタスク

「リモートアクセス VPN によるトラフィックの許可」で説明したように、トラフィックが VPN トンネルで許可されていることを確認します。

接続プロファイルのための *AAA* の設定

認証、許可、およびアカウンティング（AAA） サーバーは、ユーザー名とパスワードを使用して、ユーザーのリモートアクセス VPN へのアクセスを許可するかどうかを判断します。RADIUS サーバを使用する場合は、認証されたユーザー間で許可レベルを区別して、保護されたリソースへの差別化されたアクセスを提供できます。使用状況を追跡するためにRADIUS アカウンティングサービスを使用することもできます。

AAA を設定する場合は、プライマリ アイデンティティ ソースを設定する必要があります。セカンダリソースとフォールバックソースはオプションです。RSA トークンや DUO などを使用する二重認証を実装する場合は、セカンダリソースを使用します。

プライマリ アイデンティティ ソースのオプション

- [ユーザー認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：リモート ユーザーの認証に使用されるプライマリ アイデンティティ ソース。VPN 接続を完了するには、エンド ユーザがこのソースか任意のフォールバック ソースで定義されている必要があります。次のいずれかを選択します。
  - Active Directory（AD）のアイデンティ レルム。必要なレルムがまだ存在していない場合は、[新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックします。
  - RADIUS サーバーグループ。
  - LocalIdentitySource（ローカル ユーザー データベース）：デバイスで直接ユーザーを定義できます。外部サーバーを使用することはできません。
- [フォールバックローカルアイデンティティソース（Fallback Local Identity Source）]：プライマリソースが外部サーバーの場合、プライマリサーバーが使用できない場合のフォールバックとして LocalIdentitySource を選択できます。フォールバック ソースとしてローカル データベースを使用する場合は、必ず外部サーバで定義したものと同じローカル ユーザ名/パスワードを定義します。
- [削除オプション（Strip options）]：レルムとは管理ドメインのことです。次のオプションを有効にすると、ユーザー名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバーが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
  - [ユーザー名からアイデンティティソースサーバーを削除（Strip Identity Source Server from Username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からアイデンティティソース名を削除するかどうか。たとえば、このオプションを選択してユーザーがユーザー名として domain\username を入力すると、ドメインがユーザー名から取り除かれ、認証用に AAA サーバーに送信されます。デフォルトでは、このオプションはオフになります。
  - [ユーザー名からグループを削除（Strip Group from username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からグループを削除するかどうか。このオプションは、username@domain 形式で指定された名前に適用されます。選択すると、domain と @ 記号が削除されます。デフォルトでは、このオプションはオフになります。

セカンダリ アイデンティティ ソース

- [ユーザー認証用のセカンダリアイデンティティソース（Secondary Identity Source for User Authentication）]：オプションの 2 番目のアイデンティティソースです。ユーザーがプライマリソースで正常に認証されると、セカンダリソースでの認証が求められます。AD レル

ム、RADIUS サーバーグループ、またはローカル アイデンティティ ソースを選択することができます。

- [詳細オプション（Advanced options）]：[詳細（Advanced）] リンクをクリックし、次のオプションを設定します。
  - [セカンダリ用フォールバックローカルアイデンティティソース（Fallback Local Identity Source for Secondary）]：セカンダリソースが外部サーバーの場合、セカンダリサーバーが使用できない場合のフォールバックとして LocalIdentitySource を選択できます。フォールバックソースとしてローカルデータベースを使用する場合は、必ずセカンダリ外部サーバーで定義したものと同じローカルユーザー名/パスワードを定義します。
  - [セカンダリログインにプライマリユーザー名を使用（Use Primary Username for Secondary Login）]：デフォルトでは、セカンダリ アイデンティティ ソースを使用する場合、セカンダリ ソースに対してユーザー名とパスワードの両方が求められます。このオプションを選択すると、システムはセカンダリパスワードの入力のみを求め、プライマリ アイデンティティ ソースに対して認証されたものと同じユーザー名をセカンダリソースに対して使用します。プライマリとセカンダリの両方のアイデンティティソースで同じユーザー名を設定する場合は、このオプションを選択します。
    - [セッションサーバーのユーザー名（Username for Session Server）]：認証に成功すると、ユーザー名はイベントと統計ダッシュボードに表示されます。ユーザー名はユーザーベースまたはグループベースの SSL 復号化およびアクセス制御ルールに一致するものを判断するために使用され、アカウンティングに使用されます。2 つの認証ソースを使用しているため、ユーザーアイデンティティとして、プライマリまたはセカンダリのどちらのユーザー名を使用するのかシステムに通知する必要があります。デフォルトでは、プライマリ名が使用されます。
    - [パスワードタイプ（Password Type）]：セカンダリサーバーのパスワードを取得する方法。デフォルトは [プロンプト（Prompt）] で、ユーザーはパスワードの入力が求められることを意味します。プライマリサーバーへのユーザー認証時に入力したパスワードを自動的に使用するには、[プライマリアイデンティティソースのパスワード（Primary Identity Source Password）] を選択します。すべてのユーザーに同じパスワードを使用するには [共通パスワード（Common Password）] を選択し、[共通パスワード（Common Password）] フィールドにそのパスワードを入力します。
  - [認証サーバー（Authorization Server）]：リモートアクセス VPN ユーザーを認証するように設定された RADIUS サーバーグループです。認証の完了後、認可によって、認証済みの各ユーザーが使用できるサービスおよびコマンドが制御されます。認可は、ユーザーが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザーに対して同じアクセス権を提供します。認証のために RADIUS を構成する方法については、『RADIUS およびグループポリシーを使用したユーザーの権限および属性の制御』システムがグループポリシーで定義されているものと重複する認可属性を RADIUS サーバーから取得した場合、RADIUS 属性は、グループポリシー属性をオーバーライドすることに注意してください。

- [アカウンティングサーバー（Accounting Server）]：（オプション）リモートアクセス VPN セッションへのアカウンティングに使用する RADIUS サーバーグループ。アカウンティングは、ユーザーがアクセスしているサービスや、ユーザーが消費しているネットワークリソースの数を追跡します。FTD デバイスは、RADIUS サーバにユーザアクティビティを報告します。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

接続プロファイルのための証明書認証の設定

（注） このセクションは、**認証タイプ**が **AAA のみ**の場合には適用されません。

リモート アクセス VPN 接続を認証するために、クライアント デバイスにインストールされた証明書を使用することができます。

クライアント証明書を使用していても、セカンダリ アイデンティティ ソース、フォールバック ソース、および認証およびアカウンティングサーバーを引き続き設定できます。これらは AAA オプションです。詳細については、『RA VPN 接続プロファイルの構成』を参照してください。

以下に、証明書固有の属性を示します。これらの属性は、プライマリ アイデンティティ ソースとセカンダリ アイデンティティ ソースに対して個別に設定できます。セカンダリソースの設定はオプションです。

- [証明書のユーザー名（Username from Certificate）]：次のいずれかを選択します。
  - [マップ固有フィールド（Map Specific Field）]：証明書の要素を [プライマリフィールド（Primary Field）] および [セカンダリフィールド（Secondary Field）] の順番で使用します。デフォルトはCN（共通名）と OU（組織単位）です。組織に適したオプションを選択します。これらのフィールドを組み合わせてユーザー名が提供され、このユーザー名がイベント、ダッシュボード、さらにSSL復号とアクセス制御ルールでのマッチング目的に使用されます。
  - [DN（識別名）全体をユーザー名として使用（Use entire DN (distinguished name) as username）]：システムが自動的に DN フィールドからユーザー名を導出します。•
- [詳細オプション（Advanced options）]：（[認証タイプ（Authentication Type）] が [クライアント証明書のみ（Client Certificate Only）] の場合には適用されません）：[詳細（Advanced）] リンクをクリックし、次のオプションを設定します。
  - [ユーザーログインウィンドウの証明書からユーザー名を事前入力（Prefill username from certificate on user login window）]：ユーザーに認証を要求するときに、取得したユーザー名をユーザー名フィールドに入力するかどうか。

- [ログインウィンドウでユーザー名を非表示にする（Hide username in login window）]：[事前入力（Prefill）] オプションを選択すると、ユーザー名を非表示にできます。これは、ユーザーがパスワードプロンプトでユーザー名を編集できないことを意味します。

クライアントアドレスプール割り当ての設定

リモートアクセス VPN に接続するエンドポイントにシステムが IP アドレスを提供するための方法が必要です。AAA サーバーは、これらのアドレス、DHCP サーバー、グループポリシーで設定されている IP アドレスプール、または接続プロファイルで設定された IP アドレスプールを提供できます。システムは、この順序でこれらのリソースを試行し、使用可能なアドレスを取得すると停止し、次にアドレスをクライアントに割り当てます。このように、同時接続数が異常な場合のフェールセーフを作成するために複数のオプションを設定できます。

接続プロファイルのアドレスプールを設定するには、次の方法の 1 つ以上を使用します。

- [IPv4アドレスプール（IPv4 Address Pool）] および [IPv4アドレスプール（IPv4 Address Pool）]：まず、サブネットを指定する最大 6 つのネットワークオブジェクトを作成します。IPv4 と IPv6 に別々のプールを設定できます。次に、グループポリシーまたは接続プロファイルの [IPv4アドレスプール（IPv4 Address Pool）] および [IPv6アドレスプール（IPv6 Address Pool）] オプションで、これらのオブジェクトを選択します。IPv4 と IPv6 の両方を設定する必要はありません。サポートするアドレス方式を設定してください。また、グループポリシーと接続プロファイルの両方でプールを設定する必要もありません。グループポリシーは接続プロファイル設定をオーバーライドします。そのため、グループポリシーでプールを設定する場合は、接続プロファイルのオプションを空白のままにしてください。プールはリストの順序で使用されることに注意してください。

- [DHCPサーバー（DHCP Servers）]：まず、1 つ以上の IPv4 アドレス範囲を持つ RA VPN の DHCP サーバーを設定します（DHCP を使用して IPv6 プールを設定することはできません）。次に、DHCP サーバーの IP アドレスを使用してホスト ネットワーク オブジェクトを作成します。その後、このオブジェクトは接続プロファイルの [DHCPサーバー（DHCP Servers）] 属性で選択できます。複数の DHCP サーバーを設定することができます。DHCP サーバーに複数のアドレスプールがある場合、[DHCPスコープ（DHCP Scope）] 属性を接続プロファイルにアタッチするグループポリシーで使用して、使用するプールを選択することができます。プールのネットワークアドレスを使用して、ホスト ネットワーク オブジェクトを作成します。たとえば、DHCP プールに 192.168.15.0/24 および 192.168.16.0/24 が含まれている場合、DHCP スコープを 192.168.16.0 に設定すると、192.168.16.0/24 サブネットからのアドレスが必ず選択されるようになります。

リモート アクセス VPN によるトラフィックの許可

リモートアクセス 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** コマンドを設定すると、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 ポリシーから除外されます。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、外部ユーザーがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングできないため、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には、RA VPN 設定で [復号されたトラフィックに対するバイパスアクセスコントロールポリシー（Bypass Access Control policy for decrypted traffic）] オプションを選択します。「RA VPN 設定の作成」を参照してください。

- リモート アクセス VPN アドレス プール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、アドバンスド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。

  FDM アクセス コントロール ポリシーの設定を参照してください。

バージョン 6.4.0 を実行している FDM-Managed デバイスの AnyConnect パッケージのアップグレード

Security Cloud Control を使用して、FDM-managed デバイスで使用可能な AnyConnect パッケージをアップグレードし、RA VPN ユーザーに配布できます。

AnyConnect パッケージのアップグレードに関連した主な手順は次のとおりです。

手順

ステップ 1 Firewall Device Manager を使用して AnyConnect パッケージを削除し、パッケージの新しいバージョンをアップロードします。このタスクを実行するには、次のいずれかの方法を使用します。

- 古いパッケージを削除し、Firewall Device Manager UI から新しいパッケージをアップロードします。
- 古いパッケージを削除し、Firewall Device Manager API エクスプローラから新しいパッケージをアップロードします。

ステップ 2 Firewall Device Manager の変更をデバイスに展開します。

ステップ 3 新しい設定情報を Security Cloud Control に読み込みます。

ステップ 4 RA VPN 接続プロファイルで新しいパッケージを確認します。

前提条件

- 接続プロファイルがある少なくとも 1 つの RA VPN 設定が、すでに FDM-managed デバイスに展開されています。

- https://software.cisco.com/download/home/283000185 から必要な AnyConnect パッケージをダウンロードします。シスコでは、入手可能な最新のパッケージにアップグレードすることを推奨しています。

Firewall Device Manager を使用した必要な *AnyConnect* パッケージの *Secure Firewall Threat Defense* へのアップロード

手順

ステップ 1 ブラウザを使用して、システムのホームページを開きます。例：`https://ftd.example.com`

ステップ 2 Firewall Device Manager にログインします。

ステップ 3 **[デバイス（Device）] > [リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 4 表示ボタン  （設定表示ボタン）をクリックして、接続プロファイルの概要と接続手順を開きます。

（注）
いずれかの接続プロファイルを編集して、AnyConnect パッケージを FDM-managed デバイスにアップロードできます。

ステップ 5 [編集（Edit）] ボタンをクリックして変更を加えます。

ステップ 6 [グローバル設定（Global Settings）] 画面が表示されるまで [次へ] をクリックします。[AnyConnect パッケージ（AnyConnect Package）] には、FDM-managed デバイスで使用可能な AnyConnect パッケージが表示されます。

ステップ 7 [X] ボタンをクリックして、置き換える AnyConnect パッケージを削除します。

ステップ 8 [パッケージのアップロード（Upload Package）] をクリックし、互換性のあるパッケージのアップロードに使用する OS をクリックします。

ステップ 9 パッケージを選択したら、[開く（Open）] をクリックします。アップロードされているパッケージは Firewall Device Manager の UI で確認できます。

ステップ 10 [終了（Finish）] をクリックします。設定が保存されます。

（注）

または、Firewall Device Manager API エクスプローラを使用して、AnyConnect パッケージを削除して新しいパッケージをアップロードできます。

1. URL を、/#/api-explorer を指すように編集します（たとえば、`https://ftd.example.com/#/api-explorer`）。
2. FDM-managed デバイスからパッケージを削除します。**[AnyConnectPackageFile]** > **[削除（Delete）]** をクリックします。[objID] フィールドにパッケージ ID を入力し、[試す（TRY IT OUT!）] をクリックします。
3. AnyConnect ソフトウェア パッケージの Firepower Threat Defense デバイスへのアップロードに関するセクションで説明されている手順を実行して、新しいパッケージをアップロードします。

ステップ 11 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。このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

ステップ 12 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。

RA VPN 接続プロファイルで新しいパッケージが参照されていることを確認する

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM** をクリックします。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 [FTD] タブをクリックし、アップグレードされた AnyConnect パッケージがある FDM-managed デバイスを選択します。このデバイスは競合を報告します。

ステップ 5 アウトオブバンド変更を承認して、Security Cloud Control に保存されている設定と保留中の変更を、デバイスの実行コンフィギュレーションで上書きします。詳細については、「「競合検出」ステータスの解決」を参照してください。

ステップ 6 次の手順を実行して、新しい AnyConnect パッケージを表示します。

- **[VPN]** > **[リモートアクセスVPN（Remote Access VPN）]** をクリックします。
- この FDM-managed デバイスに関連付けられている RA VPN 設定をクリックします。
- [アクション（Actions）] の [編集（Edit）] をクリックします。新しいパッケージが [デバイス（Devices）] に表示されます。

RA VPN AnyConnect クライアントプロファイルのアップロード

リモートアクセス VPN AnyConnect クライアントプロファイルは、ファイルに保存されている設定パラメータのグループです。AnyConnect クライアントプロファイルにはさまざまな種類があり、コアクライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、AMP イネーブラ、ISE ポスチャ、ネットワークの可視性、カスタマー フィードバック エクスペリエンス プロファイル、Umbrella ローミングセキュリティ、Web セキュリティの構成設定が含まれています。

Security Cloud Control では、後でグループポリシーで使用できるオブジェクトとしてこれらのプロファイルをアップロードできます。

- [AnyConnect VPNプロファイル（AnyConnect VPN Profile）]：AnyConnect クライアントプロファイルは、VPN AnyConnect クライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーが AnyConnect クライアントの設定および詳細設定からオプションを変更できるかどうかを定義します。Security Cloud Control は XML ファイル形式をサポートします。
- [AMPイネーブラサービスプロファイル（AMP Enabler Service Profile）]：このプロファイルは AnyConnect AMP イネーブラに使用されます。リモートアクセス VPN ユーザーが VPN に接続すると、AMP イネーブラがこのプロファイルとともに FDM-managed デバイスからエンドポイントにプッシュされます。Security Cloud Control は XML および ASP ファイル形式をサポートします。
- [フィードバックプロファイル（Feedback Profile）]：カスタマー エクスペリエンス フィードバック プロファイルを追加し、このタイプを選択すると、顧客が有効にして使用している機能およびモジュールに関する情報を受信できます。Security Cloud Control は FSP ファイル形式をサポートします。
- [ISEポスチャプロファイル（ISE Posture Profile）]：AnyConnect ISE ポスチャモジュールのプロファイルファイルを追加する場合は、このオプションを選択します。Security Cloud Control は XML および ISP ファイル形式をサポートします。
- [ネットワークアクセスマネージャサービスプロファイル（Network Access Manager Service Profile）]：ネットワーク アクセス マネージャのプロファイルエディタを使用して、NAM プロファイルファイルを設定および追加します。Security Cloud Control は XML および NSP ファイル形式をサポートします。
- [ネットワーク可視性サービスプロファイル（Network Visibility Service Profile）]：AnyConnect Network Visibility Module のプロファイルファイル。NVM プロファイルエディタを使用してプロファイルを作成できます。Security Cloud Control は XML および NVMSP ファイル形式をサポートします。
- [Umbrellaローミングセキュリティプロファイル（Umbrella Roaming Security Profile）]：Umbrella ローミング セキュリティ モジュールを展開する場合は、このファイルタイプを選択する必要があります。Security Cloud Control は XML および JSON ファイル形式をサポートします。

- [Webセキュリティサービスプロファイル（Web Security Service Profile）]：Web セキュリティモジュールのプロファイルファイルを追加するときに、このファイルタイプを選択します。Security Cloud Control XML、WSO、および WSP ファイル形式をサポートします。

始める前に

適切な GUI ベースの AnyConnect プロファイルエディタを使用して、必要なプロファイルを作成します。AnyConnect セキュア モビリティ クライアント カテゴリの Cisco Software Download Center からプロファイルエディタをダウンロードし、AnyConnect の「プロファイルエディタ - Windows / スタンドアロンインストーラ（MSI）」をインストールできます。プロファイルエディタのインストーラには、スタンドアロンバージョンのプロファイルエディタが含まれています。このインストール ファイルは Windows 専用で、ファイル名は anyconnect-profileeditor-win-<version>-k9.msi です。ここで、<version> は AnyConnect のバージョンです。たとえば、anyconnect-profileeditor-win-4.3.04027-k9.msi のような名前になります。プロファイル エディタをインストールする前に、Java JRE（1.6 以降）もインストールする必要があります。

このパッケージには、Umbrella ローミング セキュリティ プロファイル エディタを除き、モジュールの作成に必要なすべてのプロファイルエディタが含まれています。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの「*AnyConnect* プロファイルエディタ」の章を参照してください。Umbrella ダッシュボードから Umbrella ローミング セキュリティ プロファイルを個別にダウンロードします。詳細については、『Cisco Umbrella User Guide』の「Umbrella ローミングセキュリティ」章の「Umbrella ダッシュボードから AnyConnect ローミング セキュリティ プロファイルをダウンロードする」セクションを参照してください。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Objects** を選択します。

ステップ 3 青色のプラス  ボタンをクリックします。

ステップ 4 **[RA VPNオブジェクト（ASA & FDM）（RA VPN Objects (ASA & FDM)）]** > **[AnyConnectクライアントプロファイル（AnyConnect Client Profile）]**をクリックします。

ステップ 5 [オブジェクト名（Object Name）] フィールドに、AnyConnect クライアントプロファイルの名前を入力します。

ステップ 6 [参照（Browse）]をクリックし、プロファイルエディタを使って作成したファイルを選択します。

ステップ 7 [開く（Open）] をクリックしてプロファイルをアップロードします。

ステップ 8 [追加（Add）] をクリックしてオブジェクトを追加します。

関連情報：

- RA VPN グループポリシーウィンドウで、クライアントモジュールを AnyConnect VPN プロファイルに関連付けます。「「新しい FTD RA VPN グループポリシーの作成」を参照してください。

（注） クライアントモジュールの関連付けは、すべての ASA バージョン、およびソフトウェアバージョン 6.7 以降を実行している FDM でサポートされています。

FDM-Managed デバイスのリモートアクセス VPN のガイドラインと制限事項

RA VPN を設定する際は、次のガイドラインと制限事項に留意してください。

- AnyConnect パッケージは、Firewall Device Manager を使用してバージョン 6.4.0 を実行している FDM-Managed デバイスに事前にロードしておく必要があります。

（注） Security Cloud Control のリモートアクセス VPN 構成ウィザードを使用して、バージョン 6.5.0 を実行している FDM-Managed デバイスに AnyConnect パッケージを個別にアップロードします。

- Security Cloud Control から RA VPN を設定する前に、以下の手順を実行します。
  - Firewall Device Manager から FDM-managed デバイスの ライセンスを登録します。
  - エクスポート制御機能を使用して Firewall Device Manager から ライセンスを有効にします。
- Security Cloud Control は、拡張アクセスリストオブジェクトをサポートしていません。Firewall Device Manager で Smart CLI を使用してオブジェクトを設定し、VPN フィルタおよび認可変更（CoA）リダイレクト ACL で使用します。
- FDM-managed デバイスから作成するテンプレートには、RA VPN 設定は含まれません。
- IP プールオブジェクトと RADIUS アイデンティティソースには、デバイス固有のオーバーライドが必要です。
- 同じ TCP ポートの同じインターフェイスに、Firewall Device Manager アクセス（管理アクセスリストの HTTPS アクセス）と AnyConnect リモートアクセス SSL VPN の両方は設定できません。たとえば、外部インターフェイスにリモート アクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。Firewall Device Manager ではこれらの機能に使用されるポートを設定できないため、同じインターフェイスに両方の機能を設定できません。
- RADIUS トークンと RSA トークンを使用して二要素認証を設定すると、ほとんどの場合、デフォルトの 12 秒の認証タイムアウトでは短すぎて正常な認証が行われません。RA VPN AnyConnect クライアントプロファイルのアップロード（126 ページ）の説明に従って、カ

スタム AnyConnect クライアントプロファイルを作成し、RA VPN 接続プロファイルに適用して、認証タイムアウト値を増やします。認証タイムアウトを 60 秒以上にすることをお勧めします。これにより、ユーザーの認証および RSA トークンの貼り付けと、トークンのラウンドトリップ検証のための十分な時間が得られます。

ユーザーがAnyConnectクライアントソフトウェアをFDM-Managedデバイスにインストールする方法

Firewall Device Manager API を使用して AnyConnect クライアント ソフトウェア パッケージを FDM-managed デバイスにアップロードし、ユーザーに配布します。「AnyConnect ソフトウェアパッケージの Firepower Threat Defense デバイスへのアップロード」を参照してください。

VPN 接続を完了するには、ユーザは AnyConnect クライアント ソフトウェアをインストールする必要があります。既存のソフトウェア配布方式を使用して、ソフトウェアを直接インストールできます。または、ユーザーが FDM-managed デバイスから AnyConnect クライアントを直接インストールできます。

（注） ソフトウェアをインストールするには、ユーザにワークステーションでの管理者権限が必要です。

ソフトウェアの最初のインストールを FDM-managed デバイスからユーザーに実行させる場合、以下の手順を実行するようにユーザーに指示します。

（注） Android および iOS のユーザは、適切な App Store から AnyConnect をダウンロードする必要があります。

手順

ステップ 1 Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。このインターフェイスは、リモート アクセス VPN を設定する際に指定します。ログインを指示するメッセージがユーザに示されます。

ステップ 2 サイトにログインします。ユーザは、リモート アクセス VPN 用に設定されたディレクトリ サーバを使用して認証されます。続行するには、ログインが正常に行われる必要があります。ログインが成功すると、システムは、必要となる AnyConnect クライアントのバージョンがインストールされているかを確認します。AnyConnect クライアントがユーザーのコンピュータにないか、下位のバージョンである場合、システムは自動的に AnyConnect ソフトウェアのインストールを開始します。インストールが終了すると、AnyConnect がリモートアクセス VPN 接続を完了します。

AnyConnect クライアント ソフトウェア バージョンの配信

AnyConnectクライアントソフトウェアの新しいバージョンをユーザーに配信するには、旧バージョンを削除せずに新しいバージョンを FDM-managed デバイスにアップロードします。AnyConnect クライアントが正常にアップロードされたら、旧バージョンを削除できます。

ユーザーが次回 VPN 接続を確立すると、AnyConnect クライアントは新しいバージョンを検出します。更新されたクライアント ソフトウェアのダウンロードとインストールを指示するメッセージが自動的に表示されます。この自動化により、ソフトウェアの配布が容易になります。

次の図は、Windows OS 用の 2 つのバージョンの AnyConnect クライアントソフトウェア（**AnyConnectWindows_3.2_BGL** と **AnyConnectWindows_4.2_BGL**）を備えた FDM-managed デバイスの例を示しています。

RA VPN AnyConnect クライアントプロファイルのアップロード

リモートアクセス VPN AnyConnect クライアントプロファイルは、ファイルに保存されている設定パラメータのグループです。AnyConnect クライアントプロファイルにはさまざまな種類があり、コアクライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、AMP イネーブラ、ISE ポスチャ、ネットワークの可視性、カスタマー フィードバック エクスペリエンス プロファイル、Umbrella ローミングセキュリティ、Web セキュリティの構成設定が含まれています。

Security Cloud Control では、後でグループポリシーで使用できるオブジェクトとしてこれらのプロファイルをアップロードできます。

- [AnyConnect VPNプロファイル（AnyConnect VPN Profile）]：AnyConnect クライアントプロファイルは、VPN AnyConnect クライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーが AnyConnect クライアントの設定および詳細設定からオプションを変更できるかどうかを定義します。Security Cloud Control は XML ファイル形式をサポートします。
- [AMPイネーブラサービスプロファイル（AMP Enabler Service Profile）]：このプロファイルは AnyConnect AMP イネーブラに使用されます。リモートアクセス VPN ユーザーが VPN

に接続すると、AMP イネーブラがこのプロファイルとともに FDM-managed デバイスからエンドポイントにプッシュされます。Security Cloud Control は XML および ASP ファイル形式をサポートします。

- [フィードバックプロファイル（Feedback Profile）]：カスタマー エクスペリエンス フィードバック プロファイルを追加し、このタイプを選択すると、顧客が有効にして使用している機能およびモジュールに関する情報を受信できます。Security Cloud Control は FSP ファイル形式をサポートします。
- [ISEポスチャプロファイル（ISE Posture Profile）]：AnyConnect ISE ポスチャモジュールのプロファイルファイルを追加する場合は、このオプションを選択します。Security Cloud Control は XML および ISP ファイル形式をサポートします。
- [ネットワークアクセスマネージャサービスプロファイル（Network Access Manager Service Profile）]：ネットワーク アクセス マネージャのプロファイルエディタを使用して、NAM プロファイルファイルを設定および追加します。Security Cloud Control は XML および NSP ファイル形式をサポートします。
- [ネットワーク可視性サービスプロファイル（Network Visibility Service Profile）]：AnyConnect Network Visibility Module のプロファイルファイル。NVM プロファイルエディタを使用してプロファイルを作成できます。Security Cloud Control は XML および NVMSP ファイル形式をサポートします。
- [Umbrellaローミングセキュリティプロファイル（Umbrella Roaming Security Profile）]：Umbrella ローミング セキュリティ モジュールを展開する場合は、このファイルタイプを選択する必要があります。Security Cloud Control は XML および JSON ファイル形式をサポートします。
- [Webセキュリティサービスプロファイル（Web Security Service Profile）]：Web セキュリティモジュールのプロファイルファイルを追加するときに、このファイルタイプを選択します。Security Cloud Control XML、WSO、および WSP ファイル形式をサポートします。

始める前に

適切な GUI ベースの AnyConnect プロファイルエディタを使用して、必要なプロファイルを作成します。AnyConnect セキュア モビリティ クライアント カテゴリの Cisco Software Download Center からプロファイルエディタをダウンロードし、AnyConnect の「プロファイルエディタ - Windows / スタンドアロンインストーラ（MSI）」をインストールできます。プロファイルエディタのインストーラには、スタンドアロンバージョンのプロファイルエディタが含まれています。このインストール ファイルは Windows 専用で、ファイル名は anyconnect-profileeditor-win-<version>-k9.msi です。ここで、<version> は AnyConnect のバージョンです。たとえば、anyconnect-profileeditor-win-4.3.04027-k9.msi のような名前になります。プロファイル エディタをインストールする前に、Java JRE（1.6 以降）もインストールする必要があります。

このパッケージには、Umbrella ローミング セキュリティ プロファイル エディタを除き、モジュールの作成に必要なすべてのプロファイルエディタが含まれています。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの「*AnyConnect*

プロファイルエディタ」の章を参照してください。Umbrella ダッシュボードから Umbrella ローミング セキュリティ プロファイルを個別にダウンロードします。詳細については、『Cisco Umbrella User Guide』の「Umbrella ローミングセキュリティ」章の「Umbrella ダッシュボードから AnyConnect ローミング セキュリティ プロファイルをダウンロードする」セクションを参照してください。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Objects** を選択します。

ステップ 3 青色のプラス ボタンをクリックします。

ステップ 4 **[RA VPNオブジェクト（ASA & FDM）（RA VPN Objects (ASA & FDM)）]** > **[AnyConnectクライアントプロファイル（AnyConnect Client Profile）]**をクリックします。

ステップ 5 [オブジェクト名（Object Name）] フィールドに、AnyConnect クライアントプロファイルの名前を入力します。

ステップ 6 [参照（Browse）]をクリックし、プロファイルエディタを使って作成したファイルを選択します。

ステップ 7 [開く（Open）] をクリックしてプロファイルをアップロードします。

ステップ 8 [追加（Add）] をクリックしてオブジェクトを追加します。

関連情報：

- RA VPN グループポリシーウィンドウで、クライアントモジュールを AnyConnect VPN プロファイルに関連付けます。「「新しい FTD RA VPN グループポリシーの作成」を参照してください。

（注） クライアントモジュールの関連付けは、すべての ASA バージョン、およびソフトウェアバージョン 6.7 以降を実行している FDM でサポートされています。

リモート アクセス VPN のライセンス要件

Firewall Device Manager から FDM-managed デバイスの ライセンスを有効化（登録）して、RA VPN 接続を設定します。デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager（SSM）アカウントに登録する必要があります。また、評価ライセンスを使用して機能を設定することはできません。

また、 ライセンスを購入して有効にする必要があります。ライセンスは、 のいずれかです。これらのライセンスは、Cisco ASA ソフトウェアベースのヘッドエンドで使用される場合、さ

まざまな機能セットを許可するように設計されていますが、FDM-managed デバイスでは同様に扱われます。

Firewall Device Manager からのライセンスの有効化の詳細については、デバイスで実行されているバージョンの Cisco Firepower Threat Defense コンフィギュレーション ガイド（Firepower Device Manager 用）[英語] の「Remote Access VPN」の章にある「Licensing Requirements for Remote Access VPN」を参照してください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html#anchor531

詳細については、*Cisco AnyConnect 発注ガイド* [英語] を参照してください。http://www.cisco.com/c/en/us/product...t-listing.html には、他のデータシートもあります。

ライセンスステータスを表示するには、次の手順を実行します。

手順

ステップ 1 左側のペインで **Security Devices** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックします。

ステップ 3 [FTD] タブをクリックして、必要なデバイスを選択します。

ステップ 4 右側の [デバイスアクション（Device Actions）] ペインで、[ライセンスの管理（Manage Licenses）] をクリックします。 ライセンスが有効な場合、[ステータス（Status ）] には [有効（Enabled）] と表示されます。

デバイス モデル別の同時 VPN セッションの最大数

デバイス モデルに基づいて、1 台のデバイスで許可される同時リモート アクセス VPN セッション数に上限が設けられます。この制限は、システムパフォーマンスが許容できないレベルまで低下しないように設計されています。これらの制限は、キャパシティ プランニングに使用します。

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firepower 2110	1,500
Firepower 2120	3,500
Firepower 2130	7,500
Firepower 2140	10,000
Firepower Threat Defense Virtual	250

RADIUS 許可の変更

RADIUS 認可変更（CoA）機能は、認証、許可、アカウンティング（AAA）セッションの属性を、セッション認証後に変更するためのメカニズムを提供します。RA VPN の重要な課題は、侵害されたエンドポイントに対して内部ネットワークを保護し、ウイルスやマルウェアの影響

を受けたときに、エンドポイントへの攻撃を修復することによって、エンドポイント自体を保護することです。エンドポイントと内部ネットワークは、RA VPN セッションの前、最中、および後のすべてのフェーズで保護する必要があります。RADIUS CoA 機能は、この目標を達成するのに役に立ちます。

Cisco Identity Services Engine（ISE）RADIUS サーバーを使用する場合は、認可変更ポリシーの適用を設定できます。AAA のユーザーまたはユーザーグループのポリシーが変更されると、ISE は CoA メッセージを FTD デバイスに送信して認証を再初期化し、新しいポリシーを適用します。Inline Posture Enforcement Point（IPEP）では、FTD デバイスによって確立された各 VPN セッションにアクセスコントロールリスト（ACL）を適用する必要はありません。

関連情報：

- FTD デバイスでの認可変更の設定

FTD デバイスでの認可変更の設定

認可変更ポリシーのほとんどは、ISE サーバーで設定されます。ただし、FTD デバイスは適切に ISE に接続するように設定する必要があります。

はじめる前に

いずれかのオブジェクトでホスト名を使用する場合は、デバイスが実行しているバージョンに向けた『Firepower Device Manager 向け Cisco Firepower Threat Defense 構成ガイド』の「システム設定」章の「**データおよび管理インターフェイス用の DNS 設定**」セクションで説明されているようにデータインターフェイスで使用する DNS サーバーを構成してください。通常、システムを完全に機能させるには、いずれにしても DNS を構成する必要があります。

手順

手順

ステップ 1 FDM-managed デバイスの Firewall Device Manager にログインします。

ステップ 2 ISE への初期接続をリダイレクトするように、拡張アクセスコントロールリスト（ACL）を設定します。リダイレクト ACL の目的は、ISE がクライアントポスチャを評価できるように、初期トラフィックを ISE に送信することです。ACL は、ISE に HTTPS トラフィックを送信しますが、ISE 宛てのトラフィックや、名前解決のために DNS サーバーに送信されるトラフィックは送信しません。リダイレクト ACL の例を次に示します。

access-list redirect extended deny ip any host <ISE server IP>

access-list redirect extended deny ip any host <DNS server IP>

access-list redirect extended deny icmp any any

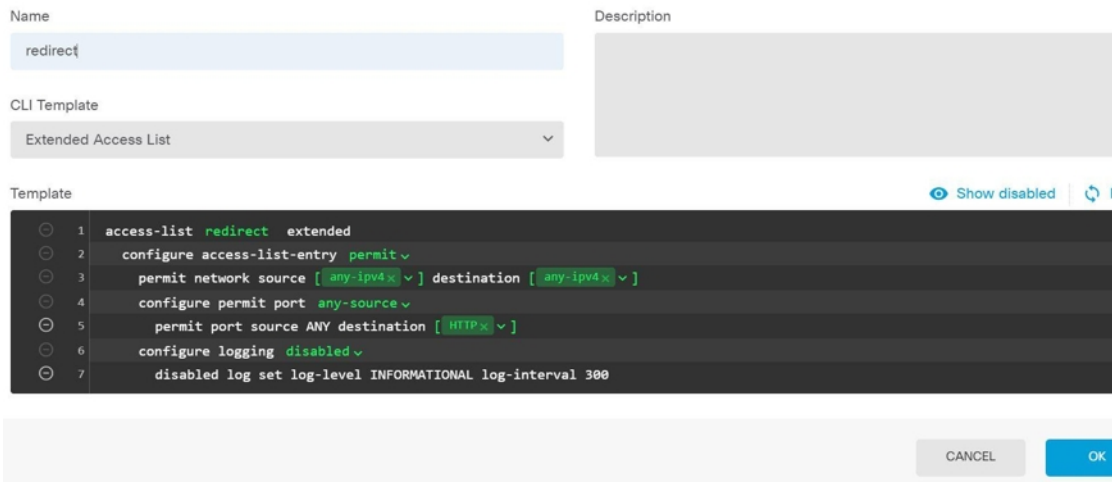
access-list redirect extended permit tcp any any eq www

ただし、ACL には、最後のアクセス制御エントリ（ACE）として暗黙の「deny any any」が含まれることに注意してください。この例では、TCP ポート www（つまりポート 80）に一致する最後の ACE は、最初の 3 つの ACE に一致するすべてのトラフィックと一致しないため、これらは冗長となります。単純に最後の ACE を使用して ACL を作成し、同じ結果を得ることも

できます。リダイレクト ACL では、permit および deny アクションによって、ACL に一致するトラフィックが特定されることに注意してください（permit は一致、deny は不一致）。トラフィックは実際にはドロップされず、拒否されたトラフィックは ISE にリダイレクトされません。リダイレクト ACL を作成するには、Smart CLI オブジェクトを設定する必要があります。

1. **[デバイス（Device）] > [詳細設定（Advanced Configuration）] > [Smart CLI] > [オブジェクト（Objects）]** を選択します。
2. [+] をクリックして新しいオブジェクトを作成します。
3. ACL の名前を入力します。たとえば、**redirect** などと入力します。
4. [CLIテンプレート（CLI Template）] の場合は、[拡張アクセスリスト（Extended Access List）] を選択します。
5. [テンプレート（Template）] 本文で次のように設定します。
   - configure access-list-entry action = permit
   - source-network = any-ipv4
   - destination-network = any-ipv4
   - configure permit port = any-source
   - destination-port = HTTP
   - configure logging = disabled

   ACE は次のようになります。



6. [OK] をクリックします。

   この ACL は、次に変更を展開するときに設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

（注）
この ACL は IPv4 にのみ適用されます。IPv6 のサポートも追加する場合は、属性がすべて同じ 2 つ目の ACE を追加します。ただし、送信元ネットワークと宛先ネットワークには

any-ipv6 を選択します。ISE または DNS サーバーへのトラフィックはリダイレクトされないようにするために、他の ACE を追加することもできます。最初に、それらのサーバーの IP アドレスを保持するホスト ネットワーク オブジェクトを作成する必要があります。

ステップ 3 RADIUS サーバーグループをダイナミック認証用に設定します。

「Firepower Threat Defense RADIUS サーバーオブジェクトまたはグループの作成または編集」セクションの説明に従って、以下の手順を実行します。

1. RADIUS サーバーオブジェクトの作成
2. RADIUS サーバーグループの作成

ステップ 4 この RADIUS サーバーグループを使用する接続プロファイルを作成します。「RA VPN 接続プロファイルの設定」を参照してください。[AAA認証（AAA Authentication）] を使用し（単独または証明書と一緒に）、[ユーザー認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]、[認可（Authorization）]、および [アカウンティング（Accounting）] オプションでサーバー グループを選択します。

FDM-Managed デバイスのリモートアクセス VPN 設定の確認

リモートアクセス VPN を設定し、設定をデバイスに展開した後で、リモート接続できることを確認します。

手順

ステップ 1 外部ネットワークから、AnyConnect クライアントを使用して VPN 接続を確立します。Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。必要に応じて、クライアント ソフトウェアをインストールし、接続を完了します。「AnyConnect クライアントソフトウェアを FTD にインストールする方法」を参照してください。グループ URL を設定した場合は、それらの URL も試みてください。

ステップ 2 [セキュリティデバイス（Security Devices）]ページで、確認するデバイスを選択し、[デバイスアクション（Device Actions）] の下にある [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 3 **show vpn-sessiondb** コマンドを使用して、現在の VPN セッションに関する概要情報を表示します。

ステップ 4 統計情報では、アクティブな AnyConnect クライアント セッション、および累積セッション数、ピーク同時セッション数、非アクティブセッション数の情報が示されます。次は、コマンドからの出力例です。

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------


   Total Active and Inactive    :      1             Total Cumulative :     50
   Device Total VPN Capacity    :  10000
   Device Load                  :     0%
   --------------------------------------------------------------------------------

   --------------------------------------------------------------------------------
   Tunnels Summary
   --------------------------------------------------------------------------------
                                 Active : Cumulative : Peak Concurrent
                                ----------------------------------------
   Clientless                   :      0 :          1 :               1
   AnyConnect-Parent            :      1 :         49 :               3
   SSL-Tunnel                   :      1 :         46 :               3
   DTLS-Tunnel                  :      1 :         46 :               3
   --------------------------------------------------------------------------------
   Totals                       :      3 :        142
   --------------------------------------------------------------------------------

   --------------------------------------------------------------------------------
   IPv6 Usage Summary
   --------------------------------------------------------------------------------
                                 Active : Cumulative : Peak Concurrent
                                ----------------------------------------
   AnyConnect SSL/TLS/DTLS      :        :           :
     Tunneled IPv6              :      1 :         20 :           2
   --------------------------------------------------------------------------------
```

ステップ 5 **show vpn-sessiondb anyconnect** コマンドを使用して、現在の AnyConnect VPN セッションに関する詳細情報を表示します。詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含まれます。VPN接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

FDM-Managed デバイスのリモートアクセス VPN 設定の詳細表示

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで、**Secure Connections** > **End User Connections** > **Remote Access VPN** > **ASA & FDM** を選択します

ステップ 3 表示された VPN 設定オブジェクトをクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

- RA VPN 設定を展開して、それらに関連付けられているすべての接続プロファイルを表示します。
  - 追加 + ボタンをクリックして新しい接続プロファイルを追加します。
  - 表示ボタン（  ）をクリックして、接続プロファイルの概要と接続手順を開きます。[アクション（Actions）] で、[編集（Edit）] をクリックして変更を変更できます。
- [アクション（Actions）] で次のオプションのいずれかをクリックすると、追加のタスクを実行できます。
  - グループポリシーを割り当て/追加するには、[グループポリシー（Group Policies）] をクリックします。
  - 不要になった設定オブジェクトまたは接続プロファイルをクリックし、[削除（Remove）] をクリックして削除します。

リモートアクセス仮想プライベート ネットワーク セッションのモニタリング

リモートアクセス仮想プライベートネットワークは、モバイルユーザーや在宅勤務者などのリモートユーザーにセキュアな接続を提供します。これらの接続をモニタリングすると、接続とユーザーセッションのパフォーマンスの重要なインジケータが一目でわかります。Security Cloud Control リモートアクセス VPN モニタリング機能を使用すると、リモートアクセス VPN の問題が存在するかどうか、およびその場所を迅速に判断できます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。また、必要に応じてリモートアクセスVPNセッションを切断できます。

[リモートアクセス仮想プライベートモニタリング（Remote Access Virtual Private Monitoring）] ページには、次の情報が表示されます。

- 最大 1 年間のアクティブなセッションと履歴セッションのリスト。
- Security Cloud Control が管理するすべてのアクティブな VPN ヘッドエンドから一目でわかるビューを提供する直感的なグラフィカルビジュアルを表示します。
- ライブセッション画面には、Security Cloud Control テナントで最も使用されているオペレーティングシステムと VPN 接続プロファイルが表示されます。また、平均セッション時間とアップロードおよびダウンロードされたデータも表示されます。
- デバイスタイプ、デバイス名、セッションの長さ、送受信されたデータ量などの基準に基づいて検索を絞り込むフィルタ処理機能。

関連情報：

- AnyConnect リモートアクセス VPN ライブセッションのモニタリング （139 ページ）
- AnyConnect リモートアクセス VPN セッション履歴のモニターリング （141 ページ）
- RA VPN セッションの検索とフィルタリング
- RA VPN モニタリングビューのカスタマイズ
- CSV ファイルへの RA VPN セッションのエクスポート
- FTD でのアクティブな RA VPN セッションの切断

AnyConnect リモートアクセス VPN ライブセッションのモニタリング

デバイス上のアクティブな AnyConnect リモートアクセス VPN セッションからのリアルタイムデータを監視できます。このデータは 10 分ごとに自動で更新されます。任意の時点でセッションの最新リストを取得するには、画面の右隅に表示されるリロードアイコン をクリックします。

始める前に

- リモートアクセス VPN ヘッドエンドの Security Cloud Control への導入準備をします。
- ライブデータを監視するデバイスの接続ステータスが、[セキュリティデバイス（Security Devices）] ページで「オンライン」になっていることを確認します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のウィンドウで、**Insights & Reports** > **Reports & Analytics** > **Remote Access Monitoring** をクリックします。

ステップ 3 [RA VPN] をクリックします。

ステップ 4 [ライブ（Live）] をクリックします。

RA VPN セッションを検索およびフィルタリングすると、デバイスタイプ、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの基準に基づいて検索を絞り込めます。

（注）
[Data TX] および [Data RX] 情報は、FTD には使用できません。

リモートアクセス VPN のライブデータの表示

ライブデータは、ダッシュボードと表形式の両方で表示されます。

[ダッシュボード（Dashboard）] ビュー

ダッシュボードを表示するには、画面の右上隅に表示される [チャートビューの表示（Show Charts View）] アイコンをクリックする必要があります。

ダッシュボードには、Security Cloud Control によって管理されるすべてのアクティブな VPN ヘッドエンドからの概要ビューが表示されます。

- [内訳（すべてのデバイス）（Breakdown (All Devices)）]：ライブセッションの合計数が表示されます。また、4 つの弧の長さに分割された円グラフも表示されます。これは、セッション数が最も多い上位 3 つのデバイスの VPN セッションの割合を示しています。残りの弧の長さは、他のデバイスの総計を表します。
- Security Cloud Control テナントで最も使用されているオペレーティングシステムと接続プロファイルが表示されます。
- 平均セッション時間とアップロードおよびダウンロードされたデータが表示されます。
- [国別のアクティブセッション（Active Sessions by Country）]：RA VPN ヘッドエンドに接続されているユーザーの場所のインタラクティブなヒートマップが表示されます。
  - 接続したユーザーの国には、その国から確立されたセッションの相対的な割合に応じて、徐々に濃い青色の陰影が付けられます。青色が濃いほど、その国から確立されたセッションが多いことを意味します。
  - マップの下部にある凡例は、国のセッション数とその国の色に使用される青の色合いとの相関関係を示すスケールが表示されます。
  - 地図上にマウスポインタを合わせると、国名と、その国から確立されたアクティブなユーザーセッションの総数が表示されます。
  - テーブルにマウスポインタを合わせると、その国の場所とアクティブなユーザーセッションの総数が地図上に表示されます。

表形式のビュー

データを表形式で表示するには、画面の右上隅にある [表形式のビューを表示（Show Tabular View）] アイコンをクリックします。

表形式のビューには、現在接続している VPN ユーザーの完全なリストが表示されます。

- [場所（Location）] 列には、パブリック IP アドレスを地理的に配置することにより、VPN ヘッドエンドに接続されているすべてのユーザーの場所が表示されます。行をクリックして、ユーザーの詳細を表示します。左ペインのロケーションリンクをクリックすると、ユーザーの場所が Google マップ上に表示されます。

重要 Security Cloud Control は、ライブデータに標準フィルタを適用し、ダッシュボードにデータを表示します。ビジュアルダッシュボードビューではカスタムフィルタがサポートされていないため、表形式のデータが表示されている場合にのみ、新しいフィルタを適用できます。適用されたすべてのフィルタを削除するには、[クリア（Clear）] をクリックします。標準フィルタは削除できません。

[RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）] 機能を使用して、デバイスタイプ、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの基準に基づいて検索を絞り込むことができます。リモートアクセス VPN セッションの検索とフィルタ処理 （143 ページ）一度に表示できる結果は最大 10,000 件です。

ステータス列の「アクティブ（Active）」ラベルの付いた緑色の点は、アクティブな VPN ユーザーのセッションを示します。

AnyConnect リモートアクセス VPN セッション履歴のモニターリング

過去 1 年間に記録された AnyConnect リモートアクセス VPN セッションの履歴データをモニタリングできます。

始める前に

- RA VPN ヘッドエンドを Security Cloud Control にオンボーディングします。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のウィンドウで、**Insights & Reports** > **Reports & Analytics** > **Remote Access Monitoring** をクリックします。

ステップ 3 [RA VPN] をクリックします。

ステップ 4 [履歴（Historical）] をクリックします。

- リモートアクセス VPN セッションデータは 1 年間保存され、クエリに使用できます。
- [RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）] 機能を使用して、デバイスタイプ、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの基準に基づいて検索を絞り込むことができます。リモートアクセス VPN セッションの検索とフィルタ処理 （143 ページ）
- [データ送信（Data TX）] および [データ受信（Data RX）] 情報は、Secure Firewall Threat Defense には使用できません。

リモートアクセス VPN の履歴データの表示

履歴データは、ダッシュボードと表形式の両方で表示されます。

[ダッシュボード（Dashboard）] ビュー

ダッシュボードを表示するには、画面の右上隅に表示される [チャートビューの表示（Show Charts View）] アイコンをクリックする必要があります。表形式のビューとともに、ダッシュボードビューが表示されます。

ダッシュボードには、Security Cloud Control によって管理されるすべてのアクティブな VPN ヘッドエンドからの概要ビューが表示されます。過去 24 時間、7 日間、および 30 日間にすべてのデバイスで記録された VPN セッションを示す棒グラフが表示されます。ドロップダウンから期間を選択できます。個々のバーにカーソルを合わせると、日付とその日の合計セッション数が表示されます。

表形式のビュー

表形式のビューのみを表示するには、画面の右上隅に表示される [表形式のビューを表示（Show Tabular View）] アイコンをクリックする必要があります。表形式には、過去 1 年間に接続した VPN ユーザーの完全なリストが表示されます。

[場所（Location）] 列には、パブリック IP アドレスを地理的に配置することにより、VPN ヘッドエンドに接続されているすべてのユーザーの場所が表示されます。行をクリックして、ユーザーの詳細を表示します。左ペインのロケーションリンクをクリックすると、ユーザーの場所が Google マップ上に表示されます。

重要 Security Cloud Control は、履歴データに標準フィルタを適用し、ダッシュボードに表示します。ダッシュボードではカスタムフィルタはサポートされていないため、表形式のデータが表示されている場合にのみ、新しいフィルタを適用できます。新たに適用されたフィルタをクリアすると、ダッシュボードが再起動します（画面で [クリア（Clear）] をクリックして、適用されたフィルタを手動で削除します）。標準フィルタは削除できません。

[RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）]リモートアクセス VPN セッションの検索とフィルタ処理 （143 ページ）機能を使用して、セッション

の日と時間の範囲、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの条件に基づいて検索を絞り込むことができます。一度に表示できる結果は最大10,000件です。

ステータス列の「アクティブ（Active）」ラベルの付いた緑色の点は、アクティブなVPNユーザーのセッションを示します。

リモートアクセス VPN セッションの検索とフィルタ処理

検索（Search）

検索バー機能を使用して、リモートアクセス VPN セッションを検索します。検索バーにデバイス名、IPアドレス、またはシリアル番号を入力し始めると、検索条件に一致するリモートアクセス VPN セッションが表示されます。検索では大文字と小文字が区別されません。

Filter

フィルタサイドバーを使用して、セッション時間の範囲、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの条件に基づいてリモートアクセス VPN セッションを特定できます。フィルタ機能は、ライブビューと履歴ビューの両方で使用できます。

- [デバイスによるフィルタ（Filter by Devices）]：1 つまたはすべてのデバイスを [すべてのタイプ（All Types）] から選択して、選択したデバイスからのセッションを表示します。このウィンドウでは、デバイスがタイプに基づいて分類され、対応するタブの下に表示されます。
- [セッションの時間範囲（Sessions Time Range）]（履歴データにのみ適用）：指定した日時範囲のセッションの履歴を表示します。表示できるのは、過去 3 ヵ月間に記録されたデータのみです。
- [セッションの長さ（Sessions Length）]：指定されたセッションの継続時間に基づいてセッションを表示します。時間の単位（時間、分、または秒）を設定し、スライダを動かして、継続時間の最小長と最大長を指定します。表示されたフィールドで長さを指定することもできます。
- [アップロード（TX）（Upload (TX)）]：セキュリティで保護されたネットワークにアップロードまたは転送されたデータの指定量に基づいてセッションを表示します。単位（GB、MB、またはKB）を設定し、スライダを適宜動かして範囲を選択します。表示されるフィールドに値を指定することもできます。
- [ダウンロード（RX）（Download (RX)）]：セキュリティで保護されたネットワークからダウンロードまたは受信したデータの指定量に基づいてセッションを表示します。単位（GB、MB、または KB）を設定し、スライダを適宜動かして範囲を選択します。表示されるフィールドに値を指定することもできます。

リモートアクセス VPN モニタリングビューのカスタマイズ

ライブモードと履歴モードの両方のリモートアクセス VPN モニタリングビューを変更して、必要なビューに適用される列ヘッダーのみを含めることができます。列の右側にある列フィルタアイコン をクリックし、必要な列を選択または選択解除します。

Security Cloud Control に次回サインインしたとき、選択した内容が Security Cloud Control に記憶されています。

RA VPN セッションの CSV ファイルへのエクスポート

1 つ以上のデバイスのリモートアクセス VPN セッションをコンマ区切り値（.csv）ファイルにエクスポートできます。Microsoft Excel などのスプレッドシート アプリケーションで .csv ファイルを開いて、リストの項目を並べ替えたり、フィルタ処理したりできます。この情報は、リモートアクセス VPN セッションの分析に役立ちます。セッションをエクスポートするたびに、Security Cloud Control は new.csv ファイルを作成します。作成されるファイルの名前には日付と時刻が含まれます。

Security Cloud Control は、最大 100,000 のアクティブセッションを CSV ファイルにエクスポートできます。すべてのデバイスからのセッションの合計数が上限を超えている場合は、[デバイス別表示（View By Device）] フィルタを使用して、個々のデバイスのレポートを生成できます。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のウィンドウで、**Insights & Reports** > **Reports & Analytics** > **Remote Access Monitoring** をクリックします。

ステップ 3 [デバイス別表示（View By Devices）] 領域で、次のいずれかを選択します。

- [すべてのデバイス（All Devices）] は、その下に一覧表示されているすべてのデバイスからアクティブセッションをエクスポートします。
- セッションをエクスポートするデバイスをクリックします。

ステップ 4 右上隅にある アイコンをクリックします。Security Cloud Control は、画面に表示されているルールを .csv ファイルにエクスポートします。

ステップ 5 スプレッドシート アプリケーションで .csv ファイルを開いて、結果を並べ替えたりフィルタリングしたりすることができます。

リモートアクセス VPN ダッシュボード

Security Cloud Control は、Cisco ASA、Cloud-Delivered Firewall Management Center 管理対象 Firewall Threat Defense、および FDM-managed デバイスからのリモートアクセス VPN 接続に関する統合情報を提供します。

1. Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。
2. 左側のペインで、[セキュアな接続（Secure Connections）]>[リモートアクセスVPN（Remote Access VPN）] の順にクリックします。

   - [VPNトンネルステータス（**VPN Tunnel Status**）]：アクティブおよびアイドル状態の VPN トンネルを表す円グラフが、それぞれ適切な色で表示されます。このチャートには、ヘッドエンド別にリモートアクセス VPN セッションの上位 10 件が示されます。
   - [統計（Statistics）]：平均セッション時間とアップロードおよびダウンロードされたデータも示されます。

FDM-Managed デバイスでのリモートアクセス VPN セッションの切断

現在は、Security Cloud Control インターフェイスを使用しても FDM-managed デバイスでリモートアクセス VPN セッションを終了できません。代わりに、SSH を使用して Firewall Threat Defense CLI に接続し、目的のユーザーを切断することができます。このタスクは、Security Cloud Control にオンボーディングされたオンライン FDM-managed デバイスで実行できます。

手順

ステップ 1 デバイスが実行しているバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の、「Getting Started」の章の「**Logging Into the Command Line Interface (CLI)**」セクションの説明に従い、Firewall Device Manager にログオンしてデバイス CLI を使用します。

ステップ 2 `vpn-sessionsdb logoff {name}` コマンドを実行します（**name** はユーザー名に置き換えます）。このコマンドは、指定したユーザー名のすべてのセッションを終了します。

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。