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、Cisco 適応型セキュリティアプライアンス（Cisco ASA）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。また、ASA 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 （1 ページ）
- 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 （37 ページ）

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。

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、ASA 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。

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。

関連情報：

- ASA 間のサイト間 VPN 設定 （3 ページ）
- ASA 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

ASA 間のサイト間 VPN 設定

Security Cloud Control は、適応型セキュリティアプライアンス（ASA）デバイスに搭載されているサイト間 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 [非同期（Not Synced）] 状態に変わります。[非同期（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。

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。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。
- 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 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：

- ASA 間のサイト間 VPN トンネルの作成 （9 ページ）

• 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
• NAT からのリモートアクセス VPN トラフィックの除外 （79 ページ）

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。

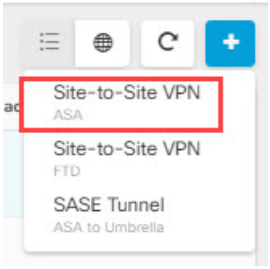
ASA 間のサイト間 VPN トンネルの作成

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 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 2 右上隅の青いプラス  をクリックし、ASA ラベル付きの [サイト間VPN] をクリックします。



ステップ 3 [設定名（Configuration name）] フィールドに、サイト間 VPN 設定の名前を入力します。

ステップ 4 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。

ステップ 5 [ピアデバイス] セクションで、次の手順を実行します。

a) [ピア1]：ASA デバイスを選択してから、[選択] をクリックします。

b) [ピア2]：他の ASA デバイスを選択してから、[選択] をクリックします。

[エクストラネット]：ピア 2 でエクストラネットデバイスを選択する場合は、[エクストラネット] スライダをクリックして有効にします。

[静的] を選択して IP アドレスを指定します。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] を選択します。[IPアドレス] 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] が表示されます。

c) [次へ（Next）] をクリックします。
d) エンドポイントデバイスの [VPNアクセスインターフェイス（VPN Access Interface）] を選択します。
e) （ルートベースの VPN に適用可能）LAN サブネットを制御する [LANインターフェイス（LAN Interfaces）] を選択します。複数のインターフェイスを選択できます。

選択した LAN インターフェイスに接続されたネットワークは、ルーティング ポリシー アクセス リストに追加されます。ルーティング ポリシー アクセス リストに一致するトラフィックは、VPN トンネルによって暗号化および復号されます。

f) [ネットワークの追加] をクリックして、参加デバイスの [保護されたネットワーク] を追加します。保護されたネットワークは、この VPN エンドポイントによって保護されるネットワークを定義します。
g) （任意かつ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 からのサイト間 VPN トラフィックの除外」を参照してください。
h) [次へ（Next）] をクリックします。

ステップ 6 （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 7 [IKE設定] セクションで、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。

ユーザーが行った構成に基づいて、Security Cloud Control は IKE 設定を提案します。推奨される IKE 構成設定を続行するか、新しい構成設定を定義することができます。

（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。

a) 必要に応じて、いずれかまたは両方の IKE バージョンを選択します。

デフォルトでは、[IKEVバージョン2] が有効になっています。

（注）

ルートベースの VPN では、IKE バージョンを両方一緒には有効にできません。

b) [IKEv2ポリシーの追加] をクリックし、IKEv2 ポリシーを選択します。

（注）
[新しいIKEv2ポリシーの作成（Create New IKEv2 Policy）] をクリックして、新しい IKEv2 ポリシーを作成します。新しい IKEv2 ポリシーの作成の詳細については、「IKEv2 ポリシーの管理」を参照してください。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。

c) 参加デバイスの [事前共有キー（Pre-Shared Key）] を入力します。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。IKE は、これらのキーを認証フェーズで使用します。

（IKEv2）[ピア1事前共有キー（Peer 1 Pre-shared Key）]、[ピア2事前共有キー（Peer 2 Pre-shared Key）]：IKEv2 の場合、各ピアで固有のキーを設定できます。[事前共有キー（Pre-shared Key）] を入力します。表示ボタンをクリックして、ピアに適切な事前共有キーを入力できます。このキーには 1 ～ 127 の英数字を指定できます。次の表で、両方のピアにおける事前共有キーの目的について説明します。

	ローカル事前共有キー	リモートピア事前共有キー
ピア 1	ピア 1 事前共有キー	ピア 2 事前共有キー
ピア 2	ピア 2 事前共有キー	ピア 1 事前共有キー

d) [IKEバージョン1（IKE Version 1）] をクリックして有効にします。

e) [IKEv1ポリシーの追加] をクリックし、IKEv1 ポリシーを選択します。[新しいIKEv1ポリシーの作成（Create New IKEv1 Policy）] をクリックして、新しい IKEv1 ポリシーを作成します。新しい IKEv1 ポリシーの作成の詳細については、「IKEv1 ポリシーの管理」を参照してください。既存の IKEv1 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。

f) （IKEv1）[事前共有キー（Pre-shared Key）]：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。このキーには 1 ～ 127 の英数字を指定できます。このシナリオでは、ピア 1 とピア 2 は同じ事前共有キーを使用してデータを暗号化および復号します。

g) [次へ（Next）] をクリックします。

ステップ 8 [IPSec設定（IPSec Settings）] セクションで、ユーザーが行った構成に基づいて、Security Cloud Control は IKEv2 プロポーザルを提案します。推奨される IKE 構成設定を続行するか、新しい構成設定を定義することができます。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。

a) [+IKEv2プロポーザル（+ IKEv2 Proposals）] をクリックして、IPSec 構成を選択します。[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。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。

（注）
[新しいIKEv2プロポーザルの作成（Create New IKEv2 Proposal）] をクリックして、新しい IKEv2 プロポーザルを作成します。新しい IKEv2 プロポーザルの作成の詳細については、「IPsec プロポーザルについて」を参照してください。

b) [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（6 ページ）」を参照してください。

c) [次へ（Next）] をクリックします。

ステップ 9 [終了（Finish）] セクションで構成に目を通し、構成に問題がない場合にのみ続行して、[送信（Submit）] をクリックしてください。

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、[インベントリ（Inventory）] ページでデバイスを選択し、[設定（Configuration）] > [差分（Diff）] を選択します。

新しいトンネルに関連付けられたデバイスに、サイト間 VPN 構成を展開するには、「構成変更の展開」セクションを参照してください。

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。

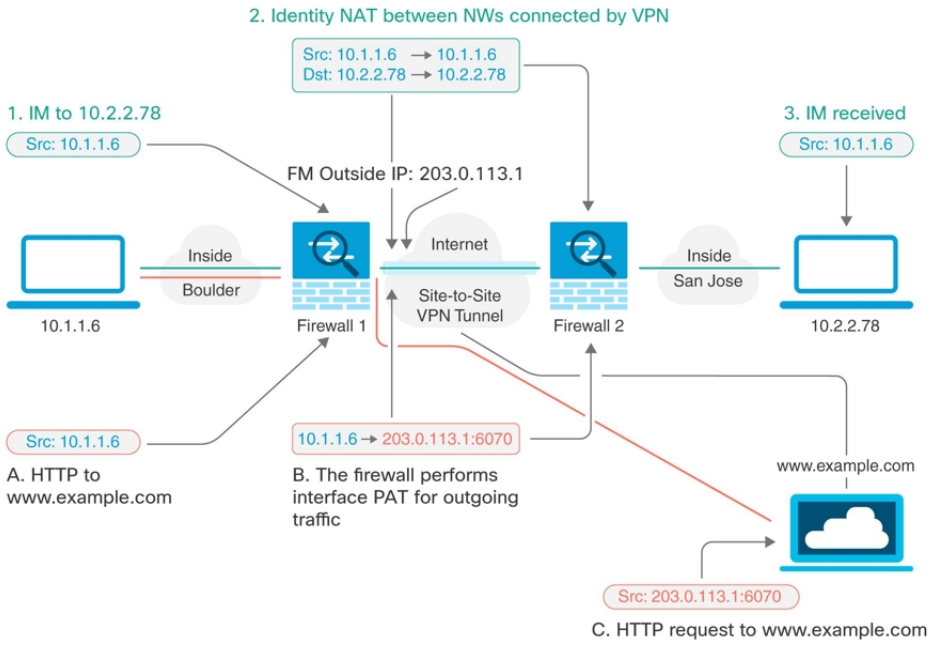
VPN 接続を作成するときに、[NATを除外（NAT Exempt）] オプションを選択すると、ルールが自動的に作成されます。ただし、これはローカルで保護されたネットワークが単一のルーテッド インターフェイス（ブリッジ グループ メンバーではない）を介して接続されている場合のみ動作します。その代わりに、接続内のローカルネットワークが複数のルーテッド インターフェイス、または 1 つ以上のブリッジ グループ メンバーの背後に存在する場合、NAT 免除ルールを手動で設定する必要があります。

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。

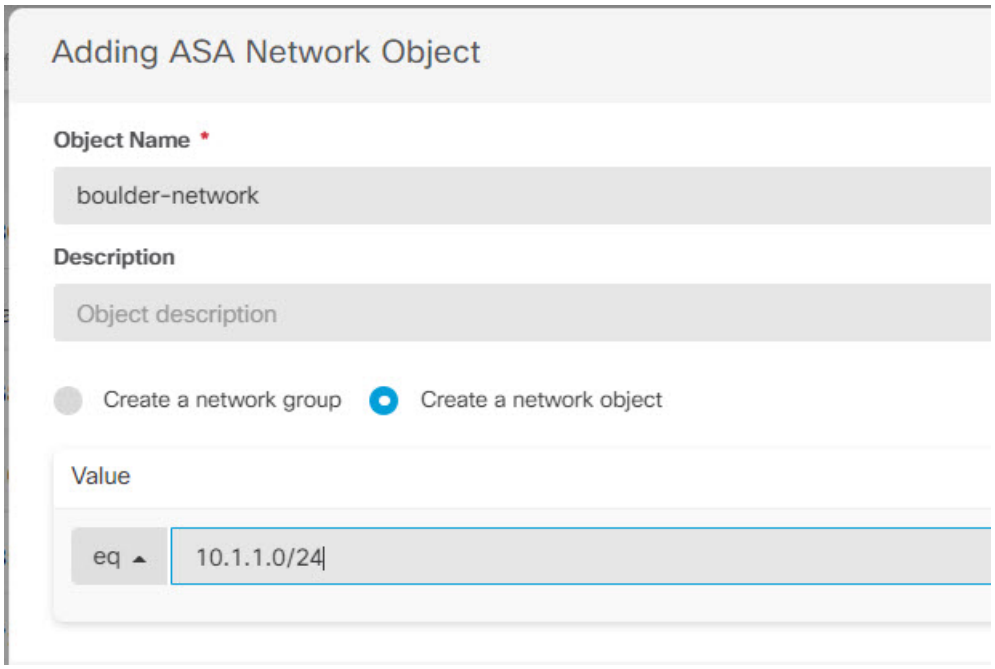
（注） この例では、IPv4 のみと仮定します。VPN に IPv6 ネットワークも含まれる場合、IPv6 にはパラレル ルールを作成します。IPv6 インターフェイス PAT は実装できないため、PAT を使用するには固有の IPv6 アドレスを持つホスト オブジェクトを作成する必要があることに注意してください。

手順

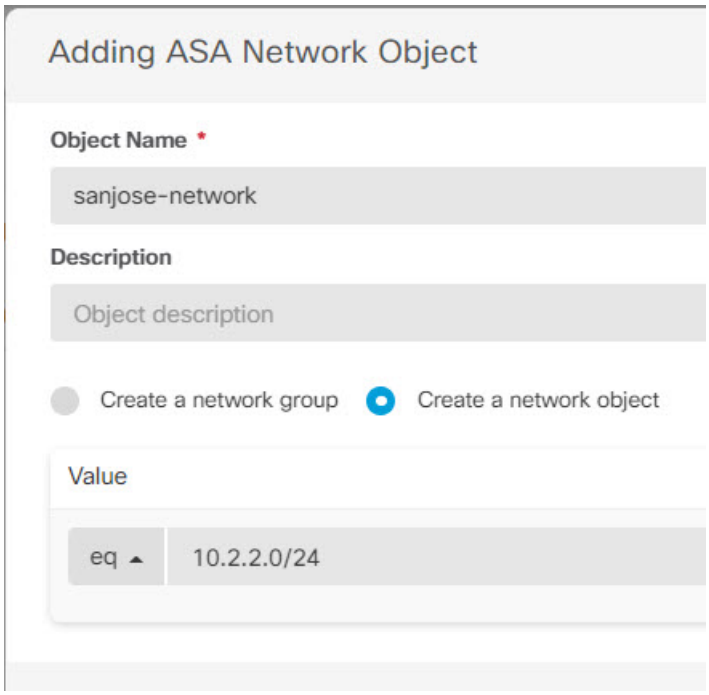
ステップ 1 さまざまなネットワークを定義するには、オブジェクトを作成します。

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. **[ASA]** > **[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。

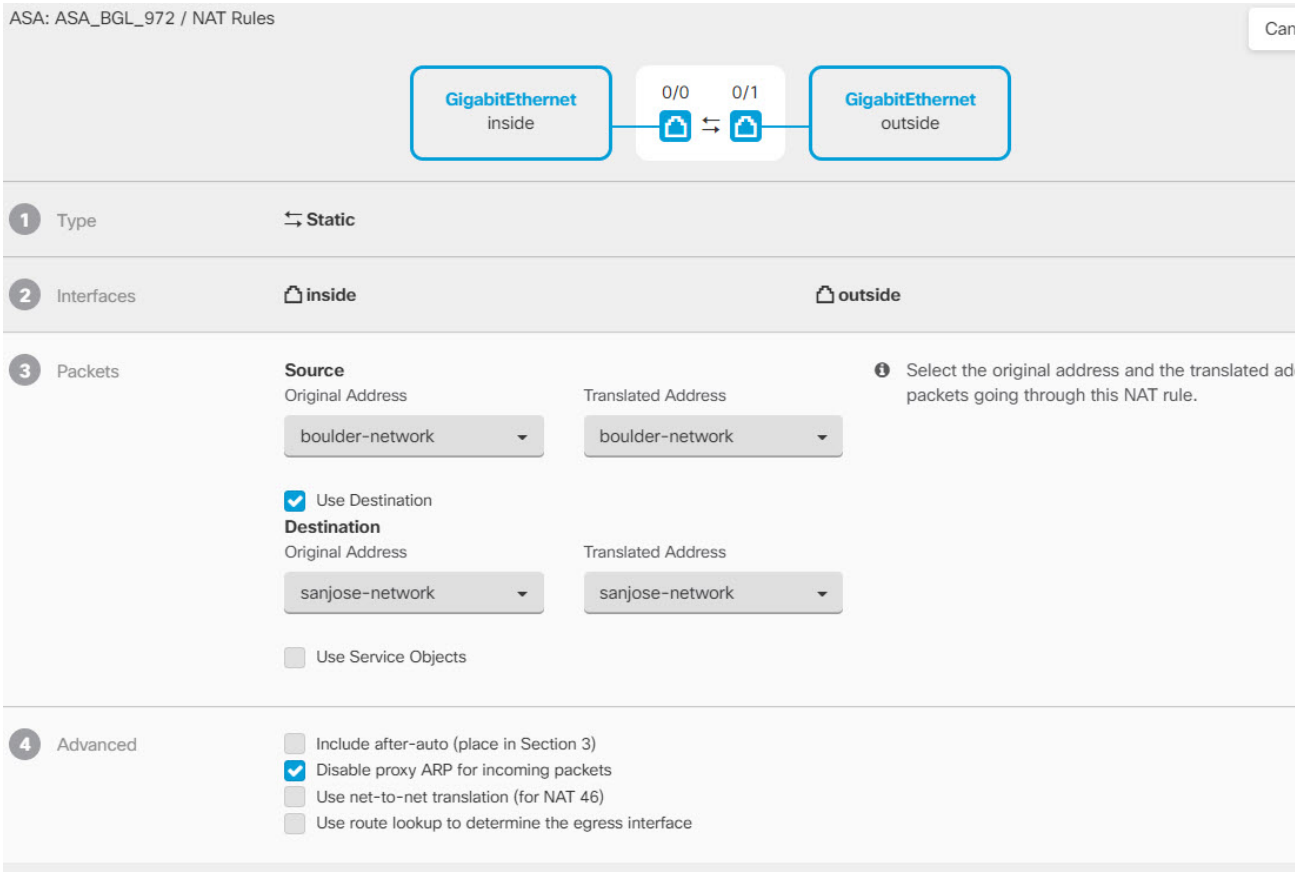


14. [追加（Add）] をクリックします。

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

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。

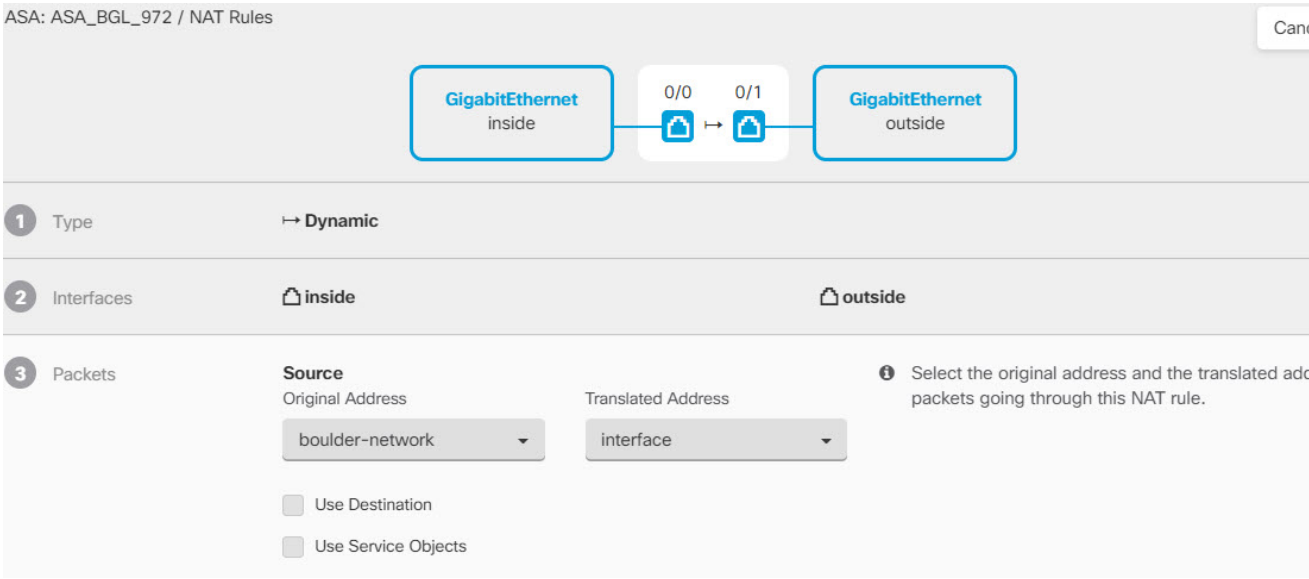


- [着信パケットのプロキシ ARP の無効化（Disable proxy ARP for incoming packets）] を選択します。
- [保存（Save）] をクリックします。
- 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 3 Firewall1（ボールダー）上でボールダーの内部ネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。注：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 4 設定変更を Security Cloud Control に展開します。詳細については、Security Cloud Control GUI を使用して行った設定変更の展開を参照してください。

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

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

Cisco ASA と Multicloud Defense Gateway 間のサイト間 VPN 設定

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。

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

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 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。

ステップ 2 右上隅にあるトンネルの作成（  ）ボタンをクリックし、**Multicloud Defense** ラベル付きの [サイト間 VPN（Site-to-Site VPN）] をクリックします。

ステップ 3 [設定名（Configuration Name）] フィールドに、作成するサイト間 VPN 設定の名前を入力します。

ステップ 4 [ピアデバイス（Peer Devices）] エリアで、次の情報を入力します。

- [デバイス1（Device 1）]：ドロップダウンリストの [Cisco ASA（ASA）] タブをクリックし、目的の Cisco ASA デバイスを選択します。
- [デバイス2（Device 2）]：ドロップダウンリストの [Multicloud Defense] タブをクリックし、目的のゲートウェイを選択します。
- [VPNアクセスインターフェイス（VPN Access Interface）]：Multicloud Defense への接続に使用する Cisco ASA インターフェイスを選択します。

- [パブリックIP（Public IP）]（任意）：選択した Cisco 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、Cisco ASA 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 5 [次へ（Next）] をクリックします。

ステップ 6 [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 [仮想トンネルインターフェイス（Virtual Tunnel Interfaces）] のアドレスを指定します。Security Cloud Control から Cisco 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）：Cisco 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 7 [次へ（Next）] をクリックします。

ステップ 8 [IKE設定（IKESettings）]エリアで、Security Cloud Control によってデフォルトの [事前共有キー（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 9 [次へ（Next）] をクリックします。

ステップ 10 [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 11 **[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。

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 ポリシーの管理
- IKEv2 ポリシーの管理

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 （21 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 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 2 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 3 [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 4 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 Diffie-Hellman 係数グループの決定」を参照してください。

ステップ 5 [追加（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 （23 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 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 2 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 3 [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 4 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 5 [追加（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。

- IPsec プロポーザルオブジェクトの管理
- 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 （26 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 左側のペインで **オブジェクト** をクリックします。

ステップ 2 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 3 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 4 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 5 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 6 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 7 [追加（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 （27 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 左側のペインで **オブジェクト** をクリックします。

ステップ 2 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 3 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 4 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 5 [追加（Add）] をクリックします。

ASA 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 ASA デバイスで既存のサイト間 VPN 設定を監視できます。サイト間の設定を変更または削除することはできません。

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 （32 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、Cisco ASA 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 左側のペインで、[VPN] > [Cisco ASA/FDMサイト間VPN（ASA/FDM Site-to-Site VPN）] の順にクリックします。**[セキュアな接続（Secure Connections）] > [サイト間VPN（Site to Site VPN）] > [ASAとFDM（ASA & FDM）]**

ステップ 2 サイト間 VPN トンネルのトンネルのリストをサイト間 VPN トンネルを検索してフィルタ処理するして、選択します。

ステップ 3 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。

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、Cisco ASA 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、または誤った設定のアクセスリストを見つける
• トンネル設定の問題を見つける
トンネル設定の問題の解決 （32 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 による管理デバイスよりも 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 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）]** をクリックして VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 4 検出された問題を確認します。

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。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 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）]** をクリックして VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 4 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 5 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 6 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 7 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 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）]** をクリックして VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 4 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 5 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 6 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 7 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 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）]** をクリックして VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 フィルタアイコン をクリックして、フィルタパネルを開きます。

ステップ 4 [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 5 問題を報告している VPN 設定を選択します。

ステップ 6 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）] **セキュリティデバイス** 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 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）]** をクリックして VPN ページを開きます。

ステップ 2 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 3 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 4 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 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）]** をクリックして VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 をクリックしてフィルタパネルを開きます。

ステップ 4 [管理対象外（Unmanaged）] にチェックを入れます。

ステップ 5 結果の表からトンネルを選択します。

ステップ 6 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。

関連情報：

- デバイスとサービスのオンボーディング
- ASA デバイスの Security Cloud Control への導入準備

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 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）]** をクリックして VPN ページを開きます。

ステップ 2 [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 3 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

手順

ステップ 1 サイト間 VPN トンネル情報の表示。
ステップ 2 [トンネルの詳細（Tunnel Details）] ペインをクリックします。
ステップ 3 [最終アクティブ確認日（Last Seen Active）] フィールドを表示します。

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 （33 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 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）]** をクリックして VPN ページを開きます。
ステップ 2 [テーブルビュー（Table View）] ボタンをクリックします。
ステップ 3 「サイト間 VPN トンネルを検索してフィルタ処理する」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。

サイト間 VPN のグローバル表示

手順

ステップ 1 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 2 [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 3 「サイト間 VPN トンネルを検索してフィルタ処理する」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 4 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 5 **[詳細の表示（View Details）]** をクリックします。

ステップ 6 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 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）]** をクリックして [VPN] ページを開きます。

ステップ 2 削除するサイト間 VPN トンネルを選択します。

ステップ 3 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：

- Cisco ASA のリモートアクセス仮想プライベートネットワークの設定 （37 ページ）

Cisco ASA のリモートアクセス仮想プライベートネットワークの設定

Cisco ASA は、ユーザーがプライベート接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することで、リモートアクセス仮想プライベートネットワーク（VPN）を構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。

セキュアな接続はトンネルと呼ばれ、ASA はトンネリング プロトコルを使用して、セキュリティパラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを介したパケットの送受信、パケットのカプセル化解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化

し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティアプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

Security Cloud Control には、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を設定するための直感的なユーザーインターフェイスがあります。また、Security Cloud Control にオンボードされた複数の適応型セキュリティアプライアンス（Cisco ASA）デバイスのリモートアクセス VPN 接続を迅速かつ簡単に設定できます。

Security Cloud Control を使用して、Cisco ASA デバイスでリモートアクセス VPN 設定をゼロから設定できます。また、Cisco Adaptive Security Defense Manager（ASDM）や Cisco Security Manager（CSM）などの他の Cisco ASA 管理ツールを使用して設定済みのリモートアクセス VPN 設定も管理できます。リモートアクセス VPN 設定がすでにある Cisco ASA デバイスをオンボードすると、Security Cloud Control は自動的に「デフォルトのリモートアクセス VPN 設定」を作成し、Cisco ASA デバイスをそ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。Security Cloud Control に読み込まれる RA VPN 属性を理解するには、「既存の Cisco ASA リモートアクセス VPN 設定の管理と展開」を参照してください。必要ない場合は、「ASA のエンドツーエンド リモート アクセス VPN 設定プロセス」で説明されている手順を実行してください。

関連情報：

- ASA のエンドツーエンド リモート アクセス VPN 設定プロセス
  - ASA のアイデンティティソースを設定する
    - ASA アクティブ ディレクトリ レルム オブジェクトの作成
    - ASA RADIUS サーバーオブジェクトまたはグループの作成
  - ASA リモートアクセス VPN グループポリシーの作成 （46 ページ）
  - Cisco ASA リモートアクセス VPN 設定の作成 （55 ページ）
  - Cisco ASA リモートアクセス VPN 接続プロファイルの設定 （60 ページ）
- 既存の Cisco ASA リモートアクセス VPN 設定の管理と展開
- IP アドレスプールの作成
- NAT からのリモートアクセス VPN トラフィックの除外 （79 ページ）
- Cisco ASA リモートアクセス VPN 設定の確認
- Cisco ASA リモートアクセス VPN 設定の詳細表示

ASA のエンドツーエンド リモート アクセス VPN 設定プロセス

このセクションでは、Security Cloud Control にオンボードされた ASA 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 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。詳細については、「ASA のアイデンティティソースを設定する」を参照してください。

次のソースを使用して、リモートアクセス VPN を使用してネットワークに接続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。「ASA アクティブ ディレクトリ レルム オブジェクトの作成」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。「ASA RADIUS サーバーオブジェクトまたはグループの作成」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：ASA デバイスで直接ユーザーアカウントを作成できるのは、Adaptive Security Device Manager（ASDM）からのみです。『Cisco ASA Series Firewall ASDM Configuration Guide, XY』の「Objects for Access Control」の章の「Configure Local User Groups」セクションを参照してください

ステップ 2 （任意）ASA リモートアクセス VPN グループポリシーの作成 （46 ページ）。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 3 Cisco ASA リモートアクセス VPN 設定の作成 （55 ページ）。

ステップ 4 Cisco ASA リモートアクセス VPN 接続プロファイルの設定 （60 ページ）。

ステップ 5 （任意）NAT からのリモートアクセス VPN トラフィックの除外 （79 ページ）。

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。

重要
Cisco Adaptive Security Device Manager（ASDM）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。「ASA 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 ASA で設定の競合を解決できます。

次のタスク

次の手順

リモートアクセス VPN 設定が ASA 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 ASA リモートアクセス VPN ヘッドエンドから、ライブ AnyConnect リモートアクセス 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 セッションのモニタリング」を参照してください。

ASA のアイデンティティソースを設定する

Microsoft Active Directory（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。

オブジェクト をクリックしてから、（  ）>[アイデンティティソース（Identity Source）] をクリック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。

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 Active Directory 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

dsquery group コマンドを入力し、ベース識別名を調べたい既知のグループ名（一部または全部）を指定します。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、Active Directory 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 で組織ユニット（OU）、グループ、ユーザーなど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します。

正しいベースであることを確認するには、次の手順を実行します。

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。問題があった場合には修正して、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（Users）] タブを選択し、ディレクトリから既知のユーザ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。ドロップダウン リストに候補が表示される場合は、システムがディレクトリに適切に照会できたことを意味します。入力した文字列がユーザ名またはグループ名として表示されることが確かであるにもかかわらず、候補が表示されない場合は、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

詳細については、「ASA アクティブ ディレクトリ レルム オブジェクトの作成」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 サーバを使用するように機能を設定する場合は、個別のサーバではなく 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 サーバの集合です。グループに複数のサーバがある場合は、それらは、1 つのサーバ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を形成します。ただし、サーバが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、「ASA RADIUS サーバーオブジェクトまたはグループの作成」を参照してください。

ASA アクティブ ディレクトリ レルム オブジェクトの作成

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 ASA デバイスに設定要求を送信します。次に ASA は、設定された AD レルムと通信します。

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 左側のペインで **オブジェクト** をクリックします。

ステップ 2 **[オブジェクトの作成（Create Object）]**（  ）**[RA VPNオブジェクト（ASAおよびFDM）（RA VPN Objects (ASA & FDM)）] > [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 3 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 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 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 6 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。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。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。

ステップ 7 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情報のダウンロードに暗号化接続を使用するには、[LDAPS] を選択し、SSL を使用して ASA と LDAP サーバー間の通信を保護します。LDAP over SSL が必要です。ポート 636 を使用します。

  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。

ステップ 8 （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 9 （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 Active Directory（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 10 [追加（Add）] をクリックします。

ASA 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 左側のペインで **オブジェクト** をクリックします。

ステップ 2 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 3 編集するオブジェクトを選択します。

ステップ 4 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 5 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 6 [保存（Save）] をクリックします。

ステップ 7 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 8 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。

ASA RADIUS サーバーオブジェクトまたはグループの作成

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 ASA デバイスに送信します。

ASA 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 左側のペインで **オブジェクト** をクリックします。

ステップ 2 [オブジェクトの作成（Create Object）]（ ）> **[RA VPNオブジェクト（ASAおよびFDM）（RA VPN Objects (ASA & FDM)）]** > **[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 3 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 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 [アイデンティティ 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 6 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。
- [サーバ秘密キー（Server Secret Key）] の入力（オプション）：ASA 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 7 [追加（Add）] をクリックします。

ステップ 8 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。

ASA 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 左側のペインで **オブジェクト** をクリックします。

ステップ 2 **[オブジェクトの作成（Create Object）]**（+）**[RA VPNオブジェクト（ASAおよびFDM）（RA VPN Objects (ASA & FDM)）] [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 3 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 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 [アイデンティティ 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 6 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 7 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 8 [RADIUS サーバーの追加（RADIUS SERVER 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、ASA 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 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。

ASA 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 左側のペインで **オブジェクト** をクリックします。

ステップ 2 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 3 編集するオブジェクトを選択します。

ステップ 4 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 5 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 6 [保存（Save）] をクリックします。

ステップ 7 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 8 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。

ASA リモートアクセス 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 オブジェクトをリモートアクセス 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リモートアクセス 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 左側のペインで **オブジェクト** をクリックします。

ステップ 2 > **[RA VPNオブジェクト（Cisco ASAおよびFDM）（RA VPN Objects (ASA & FDM)）]** > **[RA VPNグループポリシー（RA VPN Group Policy）]** をクリックします。

ステップ 3 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 4 [デバイスタイプ（Device Type）] ドロップダウンで、[ASA] を選択します。

ステップ 5 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。
  - ASA リモートアクセス VPN グループポリシー属性
  - AnyConnect クライアント プロファイル （48 ページ）
  - セッション設定属性 （49 ページ）
  - アドレス割り当て属性 （50 ページ）
  - スプリット トンネリング属性 （50 ページ）
  - AnyConnect 属性 （52 ページ）
  - トラフィック フィルタ属性 （54 ページ）
  - Windows ブラウザ プロキシ属性 （55 ページ）

ステップ 6 [保存（Save）] をクリックしてグループポリシーを作成します。

ASA リモートアクセス *VPN* グループポリシー属性

このセクションでは、ASA リモートアクセス VPN グループポリシーに関連付けられた属性について説明します。

一般属性

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。

- [DNSサーバー（DNS Server）]：VPN 接続時にドメイン名を解決するための DNS サーバーの IP アドレスを入力します。コンマを使用してアドレスを区切ることができます。
- **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）]：リモートアクセス 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

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 FTD 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 （83 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 IP アドレスプールを選択します。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。新しい IP アドレスプールの作成を作成するには、次の手順を実行します。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。**注**：同じグループポリシーで IPv4 と IPv6 両方のアドレスプールを設定できます。同じグループ ポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

- [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入力します。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入力します。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。

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、リモートアクセス 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。

はじめる前に

IPv4 ネットワーク用と IPv6 ネットワーク用のスプリットトンネルポリシーを作成する場合は、指定するアクセスリストが両方のプロトコルで使用されます。したがって、アクセスリストには、IPv4 トラフィックと IPv6 トラフィックの両方のアクセス コントロール エントリ（ACE）が含まれている必要があります。

ASA デバイスが Security Cloud Control にオンボードされると、CDO はデバイスに関連付けられた拡張 ACL を読み取ります。詳細については、「Group Policy」を参照してください。新しい ACL を作成する場合は、「ASA リスト」を参照して作成してください。

（注） 作成する ACL の送信元ネットワークとして、スプリットトンネリング用のネットワークを指定していることを確認してください。

- [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。ユーザーがリモートアクセス 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。
  - [トンネル経由の指定されたトラフィックを許可する（Allow specified traffic over the tunnel）]：送信元ネットワークを定義する拡張アクセスリストを選択します。これらの送信元から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。その他すべての送信元からのトラフィックは、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）]：送信元ネットワークを定義するネットワークオブジェクトを選択します。クライアントは、指定された送信元から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。他の送信元からのトラフィックはトンネルを通過します。

- [ネットワークリスト（Network List）]：IPv4 と IPv6 ネットワークの両方を持つことができる拡張 ACL ネットワークを選択します。

- [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。
  - [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、リモートアクセス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、リモートアクセス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、FDM 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。

Cisco ASA リモートアクセス VPN 設定の作成

Security Cloud Control を使用すると、1 つ以上の適応型セキュリティアプライアンス（Cisco ASA）デバイスをリモートアクセス 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、各リモートアクセス VPN 設定には、リモートアクセス VPN 設定に関連付けられた複数の Cisco ASA 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。

リモートアクセス VPN 設定がすでに設定されている Cisco ASA デバイス、またはリモートリモートアクセス VPN 設定のない新しいデバイスを導入準備できます。ASA デバイスの Security Cloud Control への導入準備を参照してください。リモートアクセス VPN 設定がすでにある Cisco ASA デバイスをオンボードすると、Security Cloud Control は自動的に「デフォルトのリモートアクセス VPN 設定」を作成し、Cisco ASA デバイスをそ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。詳細については、「既存の Cisco ASA リモートアクセス VPN 設定の管

理と展開」を参照してください。Security Cloud Control を使用すると、デフォルト設定を削除できます。

重要

- 同じリモートアクセス VPN 設定に ASA と FTD を追加することは許可されていません。
- 1 つの Cisco ASA デバイスに複数のリモートアクセス VPN 設定は設定できません。

始める前に

Cisco ASA デバイスをリモートアクセス VPN 設定に追加する前に、Cisco ASA デバイスで次の前提条件が満たされている必要があります。

- ライセンス要件

  輸出規制されている機能に対して、デバイスを有効にする必要があります。

  ASA デバイスのライセンスの概要を表示するには、ASA コマンドライン インターフェイスで show license summary コマンドを実行します。Security Cloud Control Cisco ASA CLI インターフェイスを使用するには、「Security Cloud Control インターフェイスでの Cisco ASA CLI の使用」を参照してください。

  - ライセンスの概要で有効になっている輸出規制機能の例：

```
Registration: Status: REGISTERED Smart Account: Cisco SVS temp-request access
licensing@cisco.com Export-Controlled Functionality: ALLOWED

Last Renewal Attempt: None

Next Renewal Attempt: Jun 08 2021 09:46:22 UTC
```

  VPN 設定を作成または編集するには、[エクスポート制御機能（Export-Controlled Functionality）] プロパティを [許可（Allowed）] ステータスにする必要があります。

  このプロパティが [許可しない（Not Allowed）] ステータスの場合、VPN 設定を作成または変更する際、Security Cloud Control がエラーメッセージ（「輸出規制に準拠していないデバイスにはリモートアクセス VPN を設定できません」）が表示され、デバイスのリモートアクセス VPN 設定は許可されません。

- デバイスのアイデンティティ証明書

  証明書は、クライアントと ASA デバイス間の接続を認証するために必要です。VPN 設定を開始する前に、アイデンティティ証明書が ASA デバイスにすでにあることを確認してください。

  証明書がデバイスにあるかどうかを確認するには、ASA コマンドライン インターフェイスで **show crypto CA Certificates** コマンドを実行します。Security Cloud Control Cisco ASA CLI インターフェイスを使用するには、「Security Cloud Control インターフェイスでの Cisco ASA CLI の使用」を参照してください。

アイデンティティ証明書がない場合、または新しい証明書に登録する場合は、Security Cloud Control を使用して証明書を Cisco ASA にインストールします。ASA 証明書管理を参照してください。

リモートアクセス VPN コンテキストでのデジタル証明書の使用については、リモートアクセス VPN 認証ベースの認証 （78 ページ）で説明されています。

- 外部インターフェイス

  外部インターフェイスが、ASA デバイスですでに設定されている必要があります。**インターフェイスを設定するには、ASDM または ASA CLI を使用する必要があります。**ASDM を使用したインターフェイスの設定については、『Cisco ASA Series General Operations CLI Configuration Guide, XY』の「Interfaces」ブックを参照してください。

- AnyConnect パッケージをダウンロードして、リモートサーバーにアップロードします。その後、リモートアクセス VPN ウィザードまたは Cisco ASA ファイル管理ウィザードを使用して、AnyConnect ソフトウェアパッケージをサーバーから Cisco ASA にアップロードします。手順については、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

- 保留中の設定展開はありません。

- 認証にローカルデータベースを使用している場合、ASDM または ASA CLI を使用して、ローカルデータベースにユーザーアカウントを追加します。

  ASDM を使用してユーザーアカウントを追加するには、『Cisco ASA Series VPN CLI Configuration Guide, X.Y』の「AAA Servers and the Local Database」ブックの「Add a User Account to the Local Database」セクションを参照してください。

  ASA CLI を使用してユーザーアカウントを追加するには、**username[***username***] password [***password***] privilege [***priv_level***]** コマンドを実行します。

- Cisco ASA の変更は Security Cloud Control に同期されます。

  1. 左側のペインで、[インベントリ（Inventory）] をクリックし、同期する 1 つ以上の Cisco ASA 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 FTD デバイスと通信して変更を同期します。

- リモートアクセス VPN 設定グループポリシーのオブジェクトには一貫性があります。

  - 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リモートアクセス VPN 設定に追加できないため、解決されていることを確認してください。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。

手順

ステップ 1 ASA デバイスの Security Cloud Control への導入準備。

ステップ 2 左側のペインで、**[VPN]** > **[Cisco ASA/FDMリモートアクセスVPN設定（ASA/FDM Remote Access VPN Configuration）]** 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、新しいリモートアクセス 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 青いプラスボタンをクリックして、ASA 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 ASA 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 ASA と FTD を追加することはできません。
   - [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。クライアントはこの証明書を承認して、セキュアな VPN 接続を完了させる必要があります。
   - [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を選択します。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インターフェイスのいずれかを選択します。

     注目
     輸出規制に準拠していないデバイスのリモートアクセス VPN 設定は作成も変更もできません。輸出規制機能が有効になっている ASA デバイスのライセンスを取得して、再試行する必要があります。

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）]：NAT 免除を使用すると、アドレスは変換から除外され、変換済みのホストとリモートホストの両方が保護されたホストとの接続を開始できるようになります。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 免除を設定します。NAT からのリモートアクセス VPN トラフィックの除外 （79 ページ）を参照してください。

3. [OK] をクリックします。

   [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] には、デバイスですでに使用可能な AnyConnect パッケージが表示されます。

   リモートアクセス VPN ウィザードから AnyConnect パッケージを Cisco ASA にアップロードするオプションは、次の 2 つです。

   - （オプション 1）：Security Cloud Control のリポジトリからパッケージを選択します。ASA はインターネットにアクセスできる必要があります。
   - （オプション 2）：AnyConnect パッケージがプリロードされている ftp/http/https/scp/smb/tftp URL の場所を指定します。

   手順については、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

   （注）
   注: 既存のパッケージを置き換える場合は、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

ステップ 6 [OK] をクリックします。

ASA VPN 設定が作成されます。

Cisco ASA リモートアクセス *VPN* 設定の変更

既存のリモートアクセス VPN 設定の名前とデバイスの詳細を変更できます。

手順

ステップ 1 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、ASA 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、既存のリモートアクセス VPN 設定を変更します。
  - [削除] をクリックして、リモートアクセス VPN 設定から Cisco ASA 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リモートアクセス 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）
    構成を使用しているデバイスがその ASA だけの場合は、ASA を削除できません。代わりに、リモートアクセス VPN 設定を削除できます。

ステップ 2 構成変更の展開

次のタスク

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：

- Cisco ASA リモートアクセス VPN 接続プロファイルの設定 （60 ページ）。

Cisco ASA リモートアクセス VPN 接続プロファイルの設定

リモートアクセス 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、リモートアクセス 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。

リモートアクセス VPN 接続プロファイルを使用すると、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。

始める前に

Cisco ASA リモートアクセス VPN 設定の作成 （55 ページ）。

手順

ステップ 1 左側のペインで、**[VPN]** > **[Cisco ASA/FDMリモートアクセスVPN設定（ASA/FDM Remote Access VPN Configuration）]** 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。

（注）
デバイスに割り当てられているグループポリシーを確認するには、[アクション（Actions）] で [グループポリシー（Group Policies）] をクリックします。接続プロファイルに割り当てられたグループポリシーは、リストに自動的に追加され、削除できません。

必要なグループポリシーがまだ存在しない場合は、  をクリックしてリストから選択します。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。ASA リモートアクセス VPN グループポリシーの作成 （46 ページ）を参照してください。

ステップ 2 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 3 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、 ASA デバイスへの接続時に、接続リストの AnyConnect クライアン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、エイリアスは Contractor、グループ URL は https://ravpn.example.com/contractor のように指定できます。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 4 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。詳細は、接続プロファイルのための AAA の設定 （62 ページ）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 5 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 6 [続行（Continue）] をクリックします。

ステップ 7 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。ASA リモートアクセス VPN グループポリシーの作成 （46 ページ）を参照してください。

ステップ 8 [続行（Continue）] をクリックします。

ステップ 9 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 10 [完了（Done）] をクリックします。

ステップ 11 「ASA のエンドツーエンド リモート アクセス VPN 設定プロセス」のステップ 5 を実行します。

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）]：認証はユーザーを特定する方法です。アクセスが許可されるには、ユーザーは通常、有効なユーザー名と有効なパスワードを入力する必要があります。プライマリ アイデンティティ ソースはリモートユーザーを認証する目的で使用されます。VPN 接続を完了するには、エンドユーザー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。
  - 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。

    ASA のアイデンティティソースを設定するをクリックすると、新しいアイデンティティソースを作成できます。

- [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「username」として domain\username に入ると、ユーザー名からドメインが削除され、認証用の AAA サーバに送信されます。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。

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。

[RADIUSサーバーグループの作成（Create RADIUS Server Group）] をクリックして、新しいサーバーグループを作成できます。ASA RADIUS サーバーオブジェクトまたはグループの作成 （44 ページ）

- [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。ASA デバイスは、RADIUS サーバーにユーザー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。

  [RADIUSサーバーグループの作成（Create RADIUS Server Group）] をクリックして、新しいサーバーグループを作成できます。ASA RADIUS サーバーオブジェクトまたはグループの作成 （44 ページ）

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Cisco ASA リモートアクセス VPN 接続プロファイルの設定 （60 ページ） を参照してください。

次に、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。新しい IPv4 または IPV6 アドレスプールを作成するには、「IP アドレスプールの作成」を参照してください。
- [DHCPサーバー（DHCP Servers）]：まず、1 つ以上の IPv4 アドレス範囲を持つリモートアクセス VPN の DHCP サーバーを設定します（IPv6 プールは DHCP を使用して設定できません）。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ASA リモートアクセス VPN グループポリシーの作成で使用して、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。

関連情報：

ASA のエンドツーエンド リモート アクセス VPN 設定プロセス

ASA デバイス上の AnyConnect ソフトウェアパッケージの管理

次のいずれかの手順を実行して、リモートアクセス VPN ウィザードを使用して AnyConnect パッケージをアップロードできます。

- Security Cloud Control リポジトリからパッケージをアップロードします。
- HTTP、HTTPS、TFTP、FTP、SMB、または SCP プロトコルを使用して、サーバーからパッケージをアップロードします。

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。

サーバーから *ASA* への *AnyConnect* パッケージのアップロード

AnyConnect クライアント ソフトウェア パッケージをコンピュータにダウンロードし、ASA からアクセス可能なリモートサーバーにそれをアップロードします。その後、RA VPN ウィザー

ドまたは ASA ファイル管理ウィザードを使用して、そのサーバーから ASA に AnyConnect ソフトウェアパッケージをアップロードします。ドメイン名を使用する URL に向けて、デバイスで DNS を正しく構成する必要があります。

ASA RA VPN ウィザードは、HTTP、HTTPS、TFTP、FTP、SMB、SCP プロトコルを使用したパッケージのアップロードをサポートしています。

ファイルのアップロード時にサポートされているプロトコルの構文:

プロトコル（Protocol）	構文	例
HTTP	http://[[パス/]ファイル名]	http://www.geonames.org/data-sources.html
HTTPS	https://[[パス/]ファイル名]	https://docs.aws.amazon.com/amazonv/tagging.html
TFTP	tftp://[[パス/]ファイル名]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[ユーザー[:パスワード]@]サーバー[:ポート]/[パス/]ファイル名]	[illegible]
SMB	smb://[[パス/]ファイル名]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[ユーザー[:パスワード]@]サーバー[/パス]/ファイル名]	scp//rootcisco123@10.10.166/root/events_send.py

始める前に

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。

重要 ASA ファイル管理ウィザードを使用してパッケージをアップロードすることを選択した場合、パッケージのダウンロード後に名前を変更しないでください。

（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サーバーにアップロードします。ASAデバイスとサーバーからのネットワークルートがあることを確認します。

ASA RA VPN ウィザードは、HTTP、HTTPS、TFTP、FTP、SMB、SCP プロトコルを使用したパッケージのアップロードをサポートしています。

重要
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。

- そのサーバーの信頼できる CA 証明書を ASA デバイスにアップロードします。
- 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。

Cisco ASA への新しい *AnyConnect* パッケージのアップロード

リモートアクセス VPN ウィザードまたは Cisco ASA ファイル管理ウィザードを使用して、AnyConnect ソフトウェアパッケージを Cisco ASA にアップロードできます。

HTTP または HTTPS サーバーから ASA デバイスに新しい AnyConnect パッケージをアップロードするには、次の手順を使用します。

手順

ステップ 1 [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 2 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 3 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。リモートアクセス VPN 設定に Cisco ASA デバイスを追加すると、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 4 [OK] をクリックします。AnyConnect パッケージがリモートアクセス VPN 設定に追加されます。

ステップ 5 ステップ 5 から、「Cisco ASA リモートアクセス VPN 設定の作成」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、「Cisco ASA の AnyConnect クライアントソフトウェアのインストール」を参照してください。

ファイル管理ウィザードを使用した *AnyConnect* パッケージのアップロード

ファイル管理ウィザードを使用して、HTTP、HTTPS、TFTP、FTP、SMB、または SCP サーバーから単一または複数の ASA デバイスに AnyConnect パッケージをアップロードします。AnyConnect パッケージを複数の ASA デバイスに同時にプッシュする場合は、一括アップロードが便利です。詳細については、「ASA ファイルの管理」を参照してください。

重要 ASA ファイル管理ウィザードを使用してパッケージをアップロードすることを選択した場合、パッケージのダウンロード後に名前を変更しないでください。

アップロードが完了したら、ASA RA VPN 設定ウィザードを開き、パッケージが自動検出されることを確認します。1 つの OS バージョンに対して複数のパッケージをアップロードする場合、ウィザードではそれらのパッケージがドロップダウンリストに表示され、そのリストの中から 1 つを選択できます。次に、RA VPN 設定を作成してデバイスに展開できます。

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、これらはリモートアクセス 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、ASA 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 左側のペインで、**[VPN] > [Cisco ASA/FDM リモートアクセス VPN（ASA/FDM Remote Access VPN）]** をクリックします。

ステップ 2 変更するリモートアクセス 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 3 [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 4 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 5 [OK] をクリックします。新しい AnyConnect パッケージがリモートアクセス VPN 設定に追加されます。

ステップ 6 ステップ 6 から、「Cisco ASA リモートアクセス VPN 設定の作成 （55 ページ）」に進みます。

AnyConnect パッケージの削除

手順

ステップ 1 左側のペインで、**[VPN]** > **[Cisco ASA/FDM リモートアクセス VPN（ASA/FDM Remote Access VPN）]** をクリックします。

ステップ 2 変更するリモートアクセス 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 3 [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を停止し、既存のパッケージが保持されます。

ステップ 4 [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）] 状態になります。

（注）
この段階で削除アクションを取り消す場合は、**セキュリティデバイス** 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 5 設定の変更を確認して、デバイスに展開します。

既存の Cisco ASA リモートアクセス VPN 設定の管理と展開

リモートアクセス VPN 設定がすでに設定されている ASDM 管理対象 Cisco ASA デバイスをオンボードすると、既存のリモートアクセス VPN 設定が検出されて表示されます。Security Cloud Control は自動的に「デフォルトのリモートアクセス VPN 設定」を作成し、Cisco ASA デバイスをこの設定に関連付けます。一部のリモートアクセス VPN 設定は、Security Cloud Control では読み取りも、サポートもされませんが、Security Cloud Control コマンドライン インターフェイスで設定できます。

（注） ここでは、Security Cloud Control でサポートされている設定またはサポートされていない設定のすべてを取り上げていません。最も一般的に使用される設定のみを説明します。

オンボーディングした Cisco ASA のリモートアクセス VPN 設定を表示するには、次の手順を実行します。

手順

ステップ 1 左側のペインで、**[VPN]** > **[Cisco ASA/FDMリモートアクセスVPN設定（ASA/FDM Remote Access VPN Configuration）]** をクリックします。

ステップ 2 オンボードされた Cisco ASA デバイスに対応するリモートアクセス VPN 設定をクリックします。Security Cloud Control は自動的に「Default_RA_VPN_Configuration」を作成し、Cisco ASA デバイスをこの設定に関連付けます。デフォルト設定は削除できます。Security Cloud Control で読み取られる Cisco ASA リモートアクセス VPN 設定は、次のように分類されます。

- デバイス設定
- 接続プロファイル
- グループ ポリシー

デバイス設定

オンボーディングされている ASA デバイスに関連付けられている RA VPN 設定が **Default_RA_VPN_Configuration** に表示されます。この設定をクリックして、この設定に関連付けられている ASA デバイス（右側の [デバイス（Devices）] ペインにあります）の名前を表示する必要があります。編集ボタンをクリックして、ASA デバイスに存在する AnyConnect パッケージを表示することもできます。

接続プロファイル

Security Cloud Control は、Cisco ASA デバイスの [AnyConnectクライアントVPNアクセス（AnyConnect Client VPN Access）] で定義された接続プロファイルをサポートしており、読み取ります。[クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] 設定はサポートしていません。

接続プロファイルの属性を確認するには、次の手順を実行します。

手順

ステップ 1 **Default_RA_VPN_Configuration** を展開します。

ステップ 2 必要な接続プロファイルの 1 つをクリックし、[編集（Edit）] をクリックします。

すべての基本および高度な Cisco ASA RA VPN 属性は、[Security Cloud Control RA VPN] 設定ページの [接続プロファイル名と詳細（Connection Profile name and details）] に表示されます。

（注） デフォルトの設定を削除できます（デフォルトの RA VPN 設定を選択し、右側の [アクション（Actions）] ペインで [削除（Remove）] をクリックします）。

プライマリ アイデンティティ ソース

- Security Cloud Control は、**接続エイリアス**と**グループ URL** 属性を**グループエイリアス、グループ URL** として読み取ります。

（注）
- SAML 、複数の証明書、複数の証明書および AAA で構成された接続プロファイルは読み取られません。
- インターフェイスとサーバーグループを持つ認証サーバーグループはサポートされていません。

- Security Cloud Control は、**プライマリ アイデンティティ ソースで**「AAA」、「AAA および証明書」、「証明書のみ」の認証方式で設定された AnyConnect 接続プロファイルをサポートします。
- **AAA サーバーグループ**は、[プライマリ アイデンティティ ソース（Primary Identity Source）] で**ユーザー認証用のプライマリ アイデンティティ ソース**として Security Cloud Control で読み取られます（この属性は、[認証タイプ（Authentication Type）] として [AAA] または [AAAとクライアント証明書（AAA and Client Certificate）] を選択することで表示できます）。
  - **AAA サーバーグループ**が LOCAL 以外に設定されている場合、Security Cloud Control はこの属性を読み取り、[プライマリ アイデンティティ ソース（Primary Identity Source）] の下の [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）] フィールドに表示します（認証タイプとして [AAA] を選択すると、この属性が表示されます）。

    Security Cloud Control で読み取られるサーバーグループ属性の詳細は、「AAA サーバグループ」を参照してください。

セカンダリ アイデンティティ ソース

[セカンダリアイデンティティソース（Secondary Identity Source）] には、ASA デバイスのセカンダリ認証属性が表示されます。これらの属性を表示するには、認証タイプとして [AAA] ま

たは [AAAおよびクライアント証明書（AAA and Client Certificate）] を選択し、[セカンダリアイデンティティソースの表示（View Secondary Identity Source）] をクリックします。

- [ユーザー認証用セカンダリアイデンティティソース（Secondary Identity Source for User Authentication）] に、セカンダリ認証の**サーバーグループ**属性が表示されます。
  - **サーバーグループ**が LOCAL 以外に設定されている場合、Security Cloud Control はこの属性を読み取り、[セカンダリ アイデンティティ ソース（Secondary Identity Source）] の下の [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）] フィールドに表示します。
- Security Cloud Control は、**属性サーバー**および**インターフェイス固有の承認サーバーグループ**属性をサポートしていません。

Security Cloud Control で読み取られるサーバーグループ属性の詳細は、「AAA サーバグループ」を参照してください。

承認サーバー

- [承認サーバー（Authorization Server）] には承認**サーバーグループ**の属性が表示されます。
- Security Cloud Control は、インターフェイスとサーバーグループを持つ承認サーバーグループをサポートしていません。

Security Cloud Control で読み取られる RADIUS サーバーグループ属性の詳細は、「RADIUS サーバグループ」を参照してください。

アカウンティングサーバー

[アカウンティングサーバー（Accounting Server）] には、アカウンティング **サーバー グループ**の属性が表示されます。Security Cloud Control で読み取られるサーバーグループ属性の詳細は、「RADIUS サーバグループ」を参照してください。

クライアントアドレスプールの割り当て

Security Cloud Control は、**クライアントアドレス割り当て属性（DHCP サーバー、クライアントアドレスプール、クライアント IPv6 アドレスプール**）をオブジェクトとして読み取ります（これらの属性は「**クライアントアドレスプールの割り当て**」で確認できます）。DHCP サーバーの詳細はリテラルとして読み取られます。

（注） Security Cloud Control は、特定のインターフェイスに割り当てられた IP アドレスプールをサポートしていません。ただし、これらの属性は ASA コマンドライン インターフェイス（CLI）で確認できます。

AAA サーバグループ

Security Cloud Control では、LDAP サーバーグループとそのグループに関連付けられた LDAP サーバーは、[Active Directoryレルム（Active Directory Realm）] オブジェクトとして表示されます。Active Directory（AD）の場合、レルムは Active Directory ドメインに相当します。Security Cloud Control は、既存の AD レルムオブジェクトの AD パスワードを読み取ります。

手順

ステップ 1 左側の Security Cloud Control ナビゲーションバーで、**オブジェクト** をクリックします。

ステップ 2 [Active Directory レルム（Active Directory レルム）] フィルタを適用して、オブジェクトを表示できます。

ステップ 3 必要な Active Directory レルムオブジェクトを選択して、[編集（Edit）] をクリックして詳細を表示します。

次のタスク

AD レルムには、関連付けられた AD サーバーとその設定が含まれていることがわかります。AD レルムに対して複数の Active Directory（AD）サーバーが存在する場合、AD サーバーは相互に複製されていて、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。これらのプロパティが同じでない場合、Security Cloud Control は Active Directory レルムオブジェクトに警告メッセージを表示します。これらのプロパティを修正して、AD サーバー全体で一貫性を持たせる必要があります。この警告に対処せずに続行すると、Security Cloud Control はいずれかの AD サーバープロパティを使用し、そのレルムオブジェクト内の他のサーバーに適用します。

RADIUS サーバグループ

ASA デバイスの AAA RADIUS サーバーグループ属性は、Security Cloud Control では RADIUS サーバー グループ オブジェクトとして読み取られます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 [RADIUSサーバーグループ（RADIUS Server Group）] フィルタを適用して、オブジェクトを確認できます。

ステップ 3 必要なオブジェクトを選択して、[編集（Edit）] をクリックして詳細を表示します。

- ASA での [ダイナミック認証の有効化（Enable dynamic authorization）]は、Security Cloud Control では [ダイナミック認証（RA VPNの場合のみ）（Dynamic Authorization (for RA VPN only)）] として読み取られます。

- [再アクティブ化モード（Reactivation Mode）] の [枯渇（Depletion）] オプションは Security Cloud Control で読み取られるため、枯渇時間に関連する [デッドタイム値（Dead Time）] も Security Cloud Control で読み取られます。ただし、[時間指定（Timed）] 属性は Security Cloud Control では読み取られません。
- Security Cloud Control は、[アカウンティングモード（Accounting Mode）]、[時間指定（Timed）]、[中間アカウンティングアップデートの有効化（Enable interim accounting update）]、[中間アカウンティングアップデートの有効化（Enable interim accounting update）]、および [認可専用モードの使用（Use authorization only mode）] をサポートしていません。

RADIUS サーバ

Security Cloud Control が Cisco ASA から RADIUS サーバーを読み取ると、「Radiusサーバーグループの名前_サーバー名またはIPアドレス」という名前を指定する RADIUS サーバーオブジェクトが作成されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。
ステップ 2 [RADIUSサーバー（RADIUS Server）] フィルタを適用して、オブジェクトを確認できます。
ステップ 3 必要なオブジェクトを選択して、[編集（Edit）] をクリックして詳細を表示します。

Group Policy

[グループポリシー（Group Policy）] セクションでドロップダウンをクリックして、デバイスに関連付けられたグループポリシーを表示します。

注目 Security Cloud Control は、トンネリングプロトコルで SSL VPN クライアントとして設定されたグループポリシーを読み取ります。

Security Cloud Control は、ASA で設定されたグループポリシー属性の大部分を読み取ります。情報は、RA VPN グループポリシーウィザードの複数のタブに渡って表示されます。ASA デバイスから読み取られたグループポリシーの詳細を表示するには、次を実行する必要があります。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。
ステップ 2 [RA VPN グループポリシー（RA VPN Group Policy）] をフィルタ処理します。

ステップ 3 そのデバイスに関連付けられているグループポリシーを選択し、[編集（Edit）] をクリックします。

次のタスク

（注） Security Cloud Control は、ASA デバイスのスプリットトンネリングで定義されている標準アクセスコントロールリスト（ACL）をサポートしていません。CDO は拡張アクセス制御リスト（ACL）をサポートし、ASA ポリシーの ACL として読み取ります。詳細については、「ASA リモートアクセス VPN グループポリシー属性」を参照してください。ポリシーを表示するには、ナビゲーションバーで [ポリシー（Policies）] > [ASA アクセスポリシー（ASA Access Policies）] をクリックします。

拡張 ACL を選択するには、次の手順を実行します。

- [スプリットトンネリング（Split Tunneling）] タブをクリックします。
- ASA のトラフィックが IPv4 または IPv6 アドレスのどちらを使用するかに基づいて、対応するドロップダウンリストから [トンネル経由の指定したトラフィックを許可する（Allow specified traffic over tunnel）] または [以下に指定したネットワークを除外する（Exclude networks specified below）] を選択します。ASA からインポートされた拡張 ACL を選択します。

IP アドレスプールの作成

ASA の IPv4 および IPv6 IP アドレスプールを設定して、VPN 接続を使用してネットワークにリモート接続しているクライアントにそれらを割り当てることができます。プールの指定順序は重要です。接続プロファイルまたはグループ ポリシーに複数のアドレス プールを設定すると、ASA は追加された順でそれらのプールを使用します。

IPv4 アドレスプールを定義するには、IP アドレス範囲を指定します。IPv4 アドレスプールの例は、10.10.147.100 - 10.10.147.177 です。

IPv6 アドレスプールを設定するには、開始 IP アドレス範囲、アドレスプレフィックス、プールに設定できるアドレス数を指定します。IPv6 アドレスプールの例は、2001:DB8:1::1 です。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

IP アドレスプールを作成するには、次の手順を実行します。

手順

ステップ 1 左側のペインで [オブジェクト（Objects）] をクリックします。

ステップ 2 青いプラスボタン をクリックし、**[ASA]** > **[アドレスプール（Address Pool）]**を選択します。

ステップ 3 [IPアドレスプールの作成（Create IP Address Pool）] ダイアログボックスで、次の情報を入力します。

- [オブジェクト名（Object Name）]：アドレスプールの名前を入力します。最大 64 文字を指定できます。
- [IPv4アドレスプール（IPv4 address pool）]：このラジオボタンを選択して、IPv4 アドレスプールを設定します。
  - [IPv4アドレス範囲（IPv4 Address Range）]：設定された各プールで使用可能な最初の IP アドレスと最後の IP アドレスを入力します。たとえば、10.10.147.100 - 10.10.147.177 です。
  - [マスク（Mask）]：この IP アドレスプールが常駐するサブネットを指定します。
- [IPv6アドレスプール（IPv6 address pool）]：このラジオボタンを選択して、IPv4 アドレスプールを設定します。
  - [IPv6 アドレス（IPv6 Address）]：設定されたプールで使用できる最初の IP アドレスとビットのプレフィックス長を、 <address>/<prefix> 形式で入力します。たとえば、2001:DB8:1::1/3 です。
  - [アドレスの数（Number of Addresses）]：IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。

ステップ 4 [保存（Save）] をクリックします。

リモートアクセス VPN 認証ベースの認証

リモートアクセス VPN は、次のシナリオでセキュアゲートウェイおよび AnyConnect クライアント（エンドポイント）を認証するためにデジタル証明書を使用します。

重要 Security Cloud Control は、VPN ヘッドエンド（Cisco ASA ）へのデジタル証明書のインストールを処理します。AnyConnect クライアントデバイスへの証明書のインストールは処理されません。これは、組織の管理者が処理する必要があります。

- VPN ヘッドエンドデバイス（ASA ）を識別して認証します。

  VPN ヘッドエンドは、AnyConnect クライアントが VPN 接続を要求するときに、VPN ヘッドエンド自体を識別して認証するためのアイデンティティ証明書を必要とします。Security Cloud Control を使用して、デバイスにアイデンティティ証明書をインストールする必要があります。「PKCS12 を使用したアイデンティティ証明書をインストールする」または「証明書とキー」を参照してください。AnyConnect クライアントに発行元の CA 証明書をインストールすることは、必須ではありません。

  Security Cloud Control からリモートアクセス VPN 設定を作成するときに、登録済みアイデンティティ証明書をデバイスの外部インターフェイスに割り当て、設定をデバイスにダウ

ンロードします。アイデンティティ証明書は、デバイスの外部インターフェイスで完全に機能するようになります。

AnyConnect クライアントが VPN への接続を試みると、デバイスは、そのアイデンティティ証明書を AnyConnect クライアントに提示することにより、それ自体を認証します。AnyConnect クライアントは、信頼できる CA 証明書を使用してこのアイデンティティ証明書を検証し、その証明書を信頼することによってデバイスを信頼します。AnyConnect クライアントに CA 証明書がインストールされていない場合、プロンプトが表示されたときに、ユーザーがデバイスを手動で信頼する必要があります。

- AnyConnect クライアントを識別して認証します。

（注） これは、リモートアクセス VPN 設定の接続プロファイルで認証方式として [クライアント証明書のみ（Client Certificate Only）] または [AAA とクライアント証明書（AAA and Client Certificate）] を使用する場合に適用されます。「AAA のみ」には適用されません。

デバイスが信頼されると、AnyConnect クライアントは、VPN 接続を完了するためにそれ自体を認証する必要があります。AnyConnect クライアントにアイデンティティ証明書をインストールし、Security Cloud Control を使用して、信頼できる CA 証明書をデバイスにインストールする必要があります。これらの証明書は、同じ認証局によって発行される必要があります。「ASA の信頼できる証明書をインストールする」を参照してください。

AnyConnect クライアントがアイデンティティ証明書を提示し、デバイスは、この証明書を信頼できる CA 証明書で検証して、VPN 接続を確立します。

NAT からのリモートアクセス VPN トラフィックの除外

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 免除を設定します。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 ルールがリモートアクセス 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。

始める前に

デバイスの接続プロファイルおよびグループポリシーで使用されるローカル IP アドレスプールの設定に一致する ASA ネットワークオブジェクトを作成します。それらのネットワークオブジェクトは、NAT ルールを設定するときに、宛先アドレスおよび変換されたアドレスとして割り当てる必要があります。「ASA ネットワークオブジェクトの作成」を参照してください。

手順

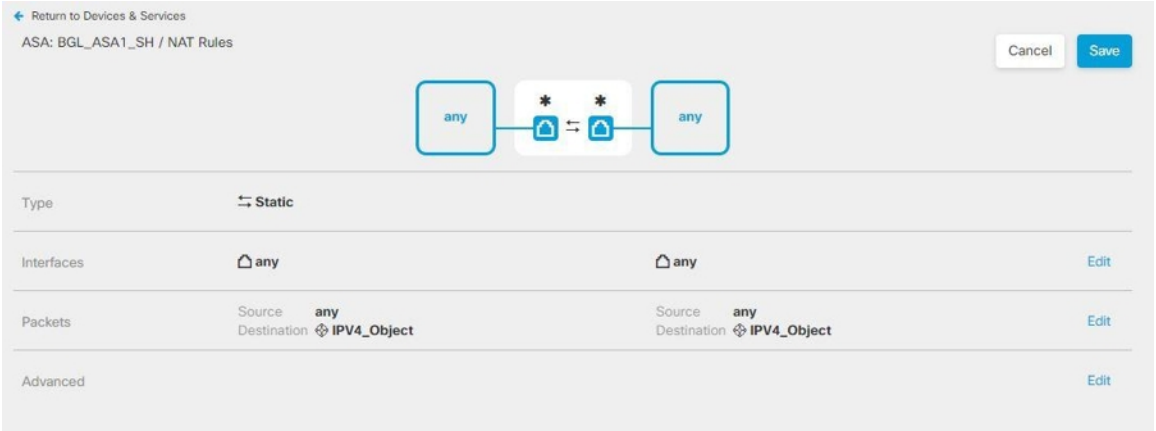
ステップ 1 左側のペインで [インベントリ（Inventory）] をクリックします。

ステップ 2 [インベントリ] フィルタと検索フィールドを使用して、NAT ルールを作成する ASA デバイスを見つけます。

ステップ 3 詳細パネルの [管理（Management）] 領域で、[NAT] NAT をクリックします。

ステップ 4 + > [Twice NAT] をクリックします。

1. 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。
2. セクション 2 で、[送信元インターフェイス（Source Interface）] で [any] および [宛先インターフェイス（Destination Interface）] で [any] を選択します。[続行（Continue）] をクリックします。
3. セクション 3 で、[送信元の元のアドレス（Source Original Address）] で [any] および [送信元の変換後アドレス（Source Translated Address）] で [any] を選択します。
4. [宛先を使用（Use Destination）] を選択します。
   1. [宛先の元のアドレス（Destination Original Address）] と [送信元の変換後アドレス（Source Translated Address）] : ドロップダウンで [選択（Choose）] をクリックし、ローカル IP アドレスプールの設定に一致するネットワークオブジェクトを選択します。次の例では、「IPV4_Object」は、ASA（BGL_ASA1_SH）デバイスの接続プロファイルおよびグループポリシー設定で使用される IPv4 アドレスプールオブジェクトと同じ設定を持つネットワークオブジェクトです。



   2. [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。

3. [保存（Save）] をクリックします。
4. プロセス（ステップ 4 から）を繰り返して、IP アドレスプールに相当する他のネットワークオブジェクトごとに同等のルールを作成します。

ステップ 5 設定の変更を確認して、デバイスに展開します。

Cisco ASA の AnyConnect クライアントソフトウェアのインストール

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、ASA デバイスから AnyConnect クライアントを直接インストールすることもできます。

（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 ASA デバイスからユーザーに行ってもらう場合、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。

Cisco ASA リモートアクセス VPN 設定の変更

Cisco ASA デバイスが Security Cloud Control にオンボードされると、オンボードされた Cisco ASA デバイスから既存のリモートアクセス VPN 設定を検出して表示します。詳細については、「既存の Cisco ASA リモートアクセス VPN 設定の管理と展開」を参照してください。

これらの設定を変更して、新しい設定をデバイスにダウンロードできます。

手順

ステップ 1 左側のペインで、[VPN] > [リモートアクセスVPN設定（Remote Access VPN Configuration）] をクリックします。

ステップ 2 グループポリシーを VPN 設定に追加または削除する場合は、オンボードの ASA デバイスに関連付けられている VPN 設定をクリックします。左側の [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。

a) 青い [+] アイコンをクリックして選択を設定し、[選択（Select）] をクリックします。

b) [保存（Save）] をクリックします。新しい ASA リモートアクセス VPN グループポリシーの作成を作成することもできます。

ステップ 3 [VPN 設定（VPN configuration）] をクリックし、[アクション（Actions）] ウィンドウで [編集（Edit）] をクリックします。

ウィザードには、設定に関連付けられている ASA デバイスが一覧表示されます。

a) 作成時と同じ方法で、次の詳細を変更できます。

- リモートアクセス VPN 設定の名前を変更します。
- デバイスの詳細が表示されている行に表示される 3 つのドットをクリックし、[編集（Edit）] をクリックします。

詳細については、Cisco ASA リモートアクセス VPN 設定の作成 （55 ページ）を参照してください。

ステップ 4 [OK] をクリックします。

ステップ 5 すべてのデバイスの設定変更のプレビューと展開

ASA 接続プロファイルの変更

手順

ステップ 1 左側のペインで、[VPN] > [リモートアクセスVPN設定（Remote Access VPN Configuration）] をクリックします。

ステップ 2 オンボードの ASA デバイスに関連付けられている VPN 設定を展開し、接続プロファイルを選択します。

ステップ 3 [アクション（Actions）] の [編集（Edit）] をクリックします。

ステップ 4 作成時と同じ方法で値を編集し、[完了（Done）] をクリックします。

詳細については、「Cisco ASA リモートアクセス VPN 接続プロファイルの設定 （60 ページ）」を参照してください。

ステップ 5 すべてのデバイスの設定変更のプレビューと展開

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 による管理 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 左側のペインで、**オブジェクト** を選択します。

ステップ 2 青色のプラス  ボタンをクリックします。

ステップ 3 **[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 4 [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 5 [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 6 [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 7 [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。「ASA リモートアクセス 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。

Cisco ASA 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。「Cisco ASA の AnyConnect クライアントソフトウェアのインストール」を参照してください。グループ URL を設定した場合は、グループ URL も試してください。

ステップ 2 [インベントリ（Inventory）] ページで、確認するデバイス（FTD または Cisco ASA）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。

ステップ 6 **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

```
> 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
```

のがわかります。

Cisco ASA リモートアクセス VPN 設定の詳細表示

手順

ステップ 1 左側のペインで、**[VPN]** > **[Cisco ASA/FDMリモートアクセスVPN設定（ASA/FDM Remote Access VPN Configuration）]** をクリックします。

ステップ 2 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。

- リモートアクセスVPN設定を展開して、設定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 （88 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 （90 ページ）
- リモートアクセス VPN セッションの検索とフィルタ処理
- 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
- RA VPN セッションの CSV ファイルへのエクスポート
- ユーザーのすべてのアクティブな 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 左側のウィンドウで、**[インサイトとレポート（Insights & Reports）]** > **[リモートアクセスのモニタリング（Remote Access Monitoring）]** をクリックします。

ステップ 2 [RA VPN] をクリックします。

ステップ 3 [ライブ（Live）] をクリックします。

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 （92 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 3 ヵ月間に記録された 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ーリングできます。

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 左側のウィンドウで、**[インサイトとレポート（Insights & Reports）]** > **[リモートアクセスのモニタリング（Remote Access Monitoring）]** をクリックします。

ステップ 2 [RA VPN] をクリックします。

ステップ 3 [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（92 ページ）
- [データ送信（Data TX）] および [データ受信（Data RX）] 情報は、Cisco 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 （92 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 左側のウィンドウで、**[インサイトとレポート（Insights & Reports）]** > **[リモートアクセスのモニタリング（Remote Access Monitoring）]** をクリックします。

ステップ 2 [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 3 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 4 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、クラウド提供型 Firewall Management Center 管理対象 脅威に対する防御、および FDM による管理 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。

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。

Cisco ASA ユーザーのリモートアクセス VPN セッションの切断

Cisco ASA デバイス上のすべてのユーザーのアクティブな RA VPN セッションを終了できます。このタスクは、ライブモードと履歴モードの両方で実行できます。

Security Cloud Control は、ユーザーが VPN セッションを表示および終了できるようにする VPN セッション マネージャ ユーザー ロールを提供します。詳細については、「ユーザーロール」を参照してください。

手順

ステップ 1 左側のウィンドウで、**[VPN] > [リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 [デバイス別表示（View By Devices）] エリアで、デバイス上のアクティブなセッションをすべて終了する [Cisco ASA（ASA）] デバイスをクリックします。

ステップ 3 右上隅に表示される [すべてのセッションを終了（Terminate All Sessions）] をクリックします。

ステップ 4 [はい、すべてのセッションを終了します（Terminate All Sessions）] をクリックして、選択を確定します。

ユーザーのすべてのアクティブな RA VPN セッションの切断

Security Cloud Control は、ユーザーを接続解除すると、ASA デバイス上のユーザーのアクティブなRA VPNセッションをすべて終了します。このタスクは、ライブモードと履歴モードの両方で実行できます。

手順

ステップ 1 左側のウィンドウで、**[VPN] > [リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 [RA VPN] タブで、[ライブ（Live）] をクリックします。

ステップ 3 セッションを切断するユーザーを検索します。[検索（Search）] バーに、検索条件を入力できます。

ステップ 4 アクティブなセッションをクリックし、右側の [アクション（Actions）] ペインで、[このユーザーのすべてのRA VPNセッションを終了する（Terminate all RA VPN sessions for this user）] リンクをクリックします。

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。