リモート アクセス VPN

リモートアクセス 仮想プライベート ネットワーク（VPN）では、各ユーザがインターネットに接続されたコンピュータまたはその他のサポート対象の iOS または Android デバイスを使用して、離れた場所からネットワークに接続することができます。これにより、モバイル ワーカーが各自のホーム ネットワークや公共の Wi-Fi ネットワークなどから接続できるようになります。

ここでは、ネットワークのリモート アクセス VPN を設定する方法について説明します。

リモート アクセス VPN の概要

Device Manager では、セキュアクライアントソフトウェアを使用して SSL 経由でリモートアクセス VPN を設定できます。

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

デバイス モデル別の同時 VPN セッションの最大数

デバイス モデルに基づいて、1 台のデバイスで許可される同時リモート アクセス VPN セッション数に上限が設けられます。この限度は、システム パフォーマンスが許容できないレベルにまで低下することがないように設定されています。キャパシティ プランニングの際は次の限度を考慮してください。

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Cisco Secure Firewall 1210CE/1210CP	200
Cisco Secure Firewall 1220CX	300
Cisco Secure Firewall 1230	500
Cisco Secure Firewall 1240	1000
Cisco Secure Firewall 1250	1500
Secure Firewall 3110	3000
Secure Firewall 3120	6000
Secure Firewall 3130	15,000
Secure Firewall 3140	20,000
Firepower 4100 シリーズ、すべてのモデル	10,000
Firepower 9300 appliance、すべてのモデル	20,000
Threat Defense Virtual: FTDv5	50
Threat Defense Virtual：FTDv10、FTDv20、FTDv30	250
Threat Defense Virtual: FTDv50	750
Threat Defense Virtual：FTDv100	10,000
ISA 3000	25

セキュアクライアント ソフトウェアのダウンロード

リモートアクセス VPN を設定するには、セキュアクライアント ソフトウェアをワークステーションにダウンロードする必要があります。VPN を定義するときに、これらのパッケージをアップロードする必要があります。

最新の機能、バグ修正、セキュリティ パッチを確保するには、最新の セキュアクライアント バージョンをダウンロードする必要があります。脅威に対する防御 デバイスのパッケージは定期的に更新してください。

（注） Windows、Mac、Linux の各オペレーティングシステムごとに 1 つの セキュアクライアント パッケージ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。

セキュアクライアント ソフトウェアパッケージは software.cisco.com から取得します。クライアントの「フル インストール パッケージ」バージョンをダウンロードしてください。

セキュアクライアント ソフトウェアのインストール方法

VPN 接続を完了するには、ユーザーは セキュアクライアント 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、Threat Defense デバイスから セキュアクライアントを直接インストールすることもできます。

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。

セキュアクライアントがすでにインストールされている場合、新しい セキュアクライアント バージョンがアップロードされると、ユーザーが次に VPN 接続を行った際、新しいバージョンが セキュアクライアント によって検出され、更新されたクライアント ソフトウェアのダウンロードとインストールを指示するメッセージが自動的に表示されます。この自動化により、ソフトウェアの配布が容易になります。

ソフトウェアの最初のインストールを Threat Defense デバイスからユーザ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に指示します。

（注） Android および iOS のユーザーは、適切な App Store から セキュアクライアント 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。

リモートアクセス VPN 接続用のポートを変更した場合、ユーザは URL にカスタムポートを含める必要があります。たとえば、ポートを 4443 に変更した場合は、https://ravpn.example.com:4443 のような URL にします。

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、必要となるセキュア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。セキュア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 セキュアクライアント 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、セキュアクライアント がリモートアクセス VPN 接続を完了します。

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

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

脅威に対する防御 デバイスは、次の順序で属性を適用します。

1. AAAサーバ上で定義されたユーザ属性: ユーザ認証や認可が成功すると、サーバからこの属性が返されます。
2. 脅威に対する防御 デバイス上で設定されているグループ ポリシー：RADIUS サーバからユーザの RADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場合は、脅威に対する防御 デバイスはそのユーザを同じ名前のグループ ポリシーに入れて、そのグループ ポリシーの属性のうち、サーバから返されないものを適用します。
3. 接続プロファイルによって割り当てられたグループポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザに適用されるデフォルトのグループポリシーが含まれています。脅威に対する防御 デバイスに接続するすべてのユーザは、最

初にこのグループに所属します。このグループでは、AAA サーバから返されるユーザ属性、またはユーザに割り当てられたグループポリシーにはない属性が定義されています。

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

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

RADIUS サーバに送信された属性

RADIUS属性146および150は、認証および許可の要求のために脅威に対する防御 デバイスからRADIUSサーバに送信されます。次の 4 つの属性はすべて、アカウンティング開始、中間アップデート、および終了の要求の場合に 脅威に対する防御 デバイスから RADIUS サーバに送信されます。

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

属性	属性番号	シンタックス、タイプ	シングルまたはマルチ値	説明または値
クライアント タイプ（Client Type）	150	整数	シングル	VPN に接続しているクライアントのタイプは次のとおりです。 2 = セキュアクライアント SSL VPN
セッション タイプ	151	整数	シングル	接続のタイプ： 1 = セキュアクライアント SSL VPN
Tunnel Group Name	146	文字列	シングル	脅威に対する防御 デバイスで定義されているセッションの確立に使用された接続プロファイルの名前。名前には 1 ～ 253 文字を使用できます。

RADIUS サーバから受信した属性

次のユーザ認可属性が 脅威に対する防御 デバイスから RADIUS サーバに送信されます。

表 *2 :* 送信される *RADIUS* 属性 *Threat Defense*

属性	属性番号	シンタックス、タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	86	文字列	シングル	アクセスリスト属性の両方が、脅威に対する防御デバイスで設定されている ACL の名前を使用します。スマート CLI 拡張アクセス リストのオブジェクト タイプを使用して、これらの ACL を作成します（**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（Smart CLI）]** > **[オブジェクト（Object）]** を選択します）。 これらのACLは、着信(脅威に対する防御 デバイスに入るトラフィック)または発信(脅威に対する防御 デバイスから出るトラフィック)方向のトラフィックフローを制御します。
Access-List-Outbound	87	文字列	シングル	
Address-Pools	217	文字列	シングル	サブネットを識別する脅威に対する防御デバイスで定義されたネットワークオブジェクトの名前。RA VPNに接続するクライアントのアドレスプールとして使用されます。[オブジェクト]ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザがログインしたときに表示されるバナー。
Banner2	36	文字列	シングル	ユーザがログインしたときに表示されるバナーの 2 番目の部分。Banner2 が Banner1 に追加されます。
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。RA VPN [グループポリシー]ページでグループポリシーを作成する必要があります。次のいずれかの形式を使用できます。 • グループポリシー名 • OU=グループポリシー名 • OU=グループポリシー名。
Simultaneous-Logins	2	整数	シングル	ユーザが確立を許可されている個別の同時接続数。0 ～ 2147483647。
VLAN	140	整数	シングル	ユーザの接続を制限する VLAN。0 ～ 4094。脅威に対する防御 デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

二要素認証

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

システムは、2 番目の要素のためにモバイルにプッシュされる RSA トークンと Duo パスコードを、ニ要素認証プロセスの最初の要素としてのRADIUSサーバまたはADサーバと組み合わせることでテストされています。

RSA 二要素認証

次のいずれかのアプローチを使用してRSAを設定できます。RSA側の設定の詳細については、RSA のマニュアルを参照してください。

- Device Manager で RADIUS サーバーとして RSA サーバーを直接定義し、RA VPN のプライマリ認証ソースとしてサーバーを使用します。

  このアプローチを使用する場合、ユーザは RSA RADIUS サーバで設定されているユーザ名を使用して認証する必要があります。また、パスワードとトークンをカンマで区切り（*password*、*token*）、パスワードと 1 回限りの一時的な RSA トークンを連結します。

  この設定では、認証サービスを提供するために（Cisco ISE で供給されるような)個別の RADIUS サーバを使用することが一般的です。2 番目の RADIUS サーバを認証サーバとして設定し、必要に応じてアカウンティングサーバを設定します。

- RSA サーバを、直接統合をサポートする RADIUS または AD サーバと統合し、プライマリ認証ソースとして非 RSA RADIUS または AD サーバを使用するように RA VPN を設定します。この場合、RADIUS/ADサーバはRSA-SDIを使用して、クライアントとRSAサーバ間の二要素認証を委任およびオーケストレーションします。

  このアプローチを使用する場合、ユーザは非 RSA RADIUS または AD サーバで設定されているユーザ名を使用して認証する必要があります。また、パスワードとトークンをカンマで区切り（*password*、*token*）、パスワードと 1 回限りの一時的な RSA トークンを連結します。

  この設定では、RSA 以外の RADIUS サーバを認証サーバとして設定し、必要に応じてアカウンティング サーバとしても設定します。

RADIUS を使用した Duo 二要素認証

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

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

次に、別の RADIUS サーバまたは AD サーバを最初の認証ファクタとして使用し、Duo クラウドサービスを 2 番目の認証ファクタとして使用するため、プロキシサーバ向けの認証要求を転送するように Duo を設定します。

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

- Duo-passcode。*my-password*,**12345** など
- push。my-password,pushなど。**push** は、ユーザによるインストールと登録が完了している Duo モバイル アプリに認証をプッシュ送信するように Duo に指示する場合に使用します。
- sms。my-password,smsなど。smsを使用して、新しいパスコードのバッチを含むSMSメッセージをユーザのモバイルデバイスに送信するようにDuoに指示します。**sms** を使用すると、ユーザの認証試行は失敗します。その後、ユーザは再認証し、2 番目の認証ファクタとして新しいパスコードを入力する必要があります。
- phone。my-password,phoneなど。**phone** は、電話コールバック認証を実行するように Duo に指示する場合に使用します。

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

LDAP を使用した Duo 二要素認証

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

脅威に対する防御 デバイスは、ポート TCP/636 経由で LDAPS を使用して、Duo LDAP と通信します。

Duo LDAP サーバは認証サービスのみを提供し、アイデンティティサービスを提供しないことに注意してください。そのため、プライマリ認証ソースとして Duo LDAP を使用する場合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザ名は表示されず、これらのユーザに対してアクセス コントロール ルールを作成することはできません。

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

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

Duo LDAP の詳細な説明と例については、Duo LDAP を使用した二要素認証の設定方法 （50 ページ）を参照してください。

リモート アクセス VPN のライセンス要件

リモート アクセス VPN を設定可能にするには、基本デバイス ライセンスがエクスポート要件を満たす必要があります。デバイスの登録は、輸出規制機能が有効化された Smart Software Manager アカウントで行う必要があります。また、評価ライセンスを使用して機能を設定することはできません。

さらに、次のいずれかのリモートアクセス VPN ライセンスを購入し、有効にする必要があります：Secure Client Advantage、Secure Client Premier、Secure Client VPN のみ。これらのライセンスは、ASA ソフトウェアベースのヘッドエンドで使用される場合、さまざまな機能セットを許可するように設計されていますが、Threat Defense デバイスでは同様に扱われます。

ライセンスを有効にするには、**[デバイス（Device）]**>**[スマートライセンス（Smart License）]**>**[設定の表示（View Configuration）]** を選択し、[RA VPNライセンス（RA VPN License）] グループで適切なライセンスを選択します。Smart Software Manager Account で使用可能なライセンスが必要です。ライセンスの有効化の詳細については、オプション ライセンスのイネーブル化とディセーブル化を参照してください。

詳細については、『Cisco AnyConnect Ordering Guide』（http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf）を参照してください。http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.htmlには、使用できるその他のデータシートもあります。

リモート アクセス VPN に関する注意事項と制限事項

RA VPN を設定する際は、次の注意事項と制限事項に注意してください。

- 同じ TCP ポートの同じインターフェイスで、Device Manager アクセス（管理アクセスリストの HTTPS アクセス）とリモートアクセス SSL VPN の両方を設定することはできません。たとえば、外部インターフェイスにリモートアクセス SSL VPN を設定する場合、ポー

ト 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。同じインターフェイスで両方の機能を設定する場合は、競合を回避するために、必ず、これらのサービスの少なくとも 1 つの HTTPS ポートを変更してください。

- RA VPN 外部インターフェイスはグローバル設定です。異なるインターフェイスに個別の接続プロファイルを設定することはできません。
- NAT ルールの送信元アドレスとリモート アクセス VPN アドレス プールの重複アドレスは使用できません。
- RADIUS トークンと RSA トークンを使用して二要素認証を設定すると、ほとんどの場合、デフォルトの 12 秒の認証タイムアウトでは短すぎて正常な認証が行われません。クライアント プロファイルの設定およびアップロード （12 ページ）で説明しているように、カスタム セキュアクライアントプロファイルを作成し、それを RA VPN 接続プロファイルに適用することにより、認証タイムアウト値を増やすことができます。認証タイムアウトを 60 秒以上にすることをお勧めします。これにより、ユーザーの認証および RSA トークンの貼り付けと、トークンのラウンドトリップ検証のための十分な時間が得られます。
- RA VPN ヘッドエンドなどに対する **curl** などのコマンドの実行は直接サポートされていないため、望ましい結果が得られない可能性があります。たとえば、ヘッドエンドは HTTP HEAD リクエストに応答しません。
- RA VPN の場合、他の属性が異なっていても、同じアイデンティティ プロバイダー（IDP）エンティティ ID URL を持つ複数の SAML サーバーオブジェクトを使用することはできません。エンティティ ID は、RA VPN 接続プロファイルで使用されるすべての SAML サーバー オブジェクトで一意である必要があります。

リモート アクセス VPN の設定

クライアントのリモート アクセス VPN を有効化するには、いくつかの項目を設定する必要があります。次の手順を実行します。

手順

ステップ 1 ライセンスを設定します。

次の 2 つのライセンスを有効にする必要があります。

- デバイスの登録は、輸出規制機能が有効化された Smart Software Manager アカウントで行う必要があります。リモート アクセス VPN を設定するには、その前に基本ライセンスが輸出規制要件を満たす必要があります。また、この機能の設定に評価ライセンスを使用することはできません。デバイスを登録する手順については、デバイスの登録を参照してください。

- リモート アクセス VPN ライセンス。詳細については、『リモート アクセス VPN のライセンス要件 （9 ページ）』を参照してください。ライセンスを有効にするには、オプション ライセンスのイネーブル化とディセーブル化を参照してください。

ステップ 2 証明書を設定します。

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

認証に使われるディレクトリ レルムに暗号化接続を使用する場合は、信頼される CA 証明書をアップロードする必要があります。

証明書とそれらのアップロード方法の詳細については、証明書の設定を参照してください。

ステップ 3 （オプション）TLS/SSLを設定します。

デフォルトでは、システムは、システムでサポートされている任意のTLSバージョンと暗号化方式を使用して、リモートユーザがリモートアクセスVPNに接続できるようにします。ただし、よりセキュアな接続を実現するため、許可されるTLS/DTLSバージョン、暗号、およびDiffie-Hellmanグループを制限することもできます。TLS/SSL暗号設定の設定を参照してください。

ステップ 4 （オプション） クライアント プロファイルの設定およびアップロード （12 ページ）.

ステップ 5 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。

リモートアクセスVPNへのログインを許可されるユーザアカウントに次のソースを使用できます。代わりに、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、認証に使用することができます。

- 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。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。
- RADIUS サーバ 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。認可およびアカウンティングにも。「RADIUS サーバ グループの設定」を参照してください。
- LocalIdentitySource（ローカル ユーザ 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。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、必ず外部サーバで定義したものと同じユーザ名/パスワードを定義します。ローカル ユーザの設定を参照してください。
- Duo LDAPサーバ: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ます。Duo LDAP サーバをプライマリ ソースとして使用することはできますが、通常の設定ではありません。通常は、プライマリ Active Directory または RADIUS サーバとともに二要素認証を提供するためのセカンダリ ソースとして使用します。詳細は、Duo LDAP を使用した二要素認証の設定方法 （50 ページ）を参照してください。
- **SAML**：プライマリ認証でSAML サーバーを使用します。SAML を使用する場合は、フォールバックまたはセカンダリ認証ソースを設定できません。詳細については、「SAML サーバの設定」を参照してください。

ステップ 6 （オプション）。 RA VPN のグループ ポリシーの設定 （29 ページ）

グループポリシーは、ユーザ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することもできます。

ステップ 7 RA VPN 接続プロファイルの設定 （19 ページ）。

ステップ 8 リモート アクセス VPN 経由のトラフィックの許可 （15 ページ）。

ステップ 9 リモート アクセス VPN 設定の確認 （16 ページ）を確認してください。

接続の完了に関する問題が発生した場合は、リモート アクセス VPN のトラブルシューティング （37 ページ）を参照してください。

ステップ 10 （オプション）アイデンティティ ポリシーを有効にして、パッシブ認証のルールを設定します。

パッシブ ユーザ認証を有効にすると、リモート アクセス VPN 経由でログインするユーザがダッシュボードに表示され、ポリシー内のトラフィック一致基準としても使用できます。パッシブ認証を有効にしない場合、RA VPN ユーザはアクティブ認証ポリシーに一致する場合にのみ使用できます。ダッシュボードのユーザ情報またはトラフィック照合用のユーザ情報を取得するには、アイデンティティ ポリシーを有効にする必要があります。

クライアント プロファイルの設定およびアップロード

セキュアクライアントプロファイルは、セキュア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、エンドユーザーがセキュア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することを許可するかどうかを定義します。

リモートアクセスVPN接続を設定する際に外部インターフェイスの完全修飾ホスト名（FQDN）を設定すると、システムが自動的にクライントプロファイルを作成します。このプロファイルでは、デフォルトの設定が有効にされます。クライントプロファイルを作成してアップロードする必要があるのは、デフォルト以外の動作が必要な場合のみです。クライントプロファイルはオプションであることに注意してください。クライントプロファイルをアップロードしなければ、セキュアクライアントはプロファイルで制御されるすべてのオプションにデフォルトの設定を使用します。

（注） 初回の接続時に、ユーザーが制御できる設定のすべてをセキュアクライアントに表示させるには、VPN プロファイルのサーバーリストに、Threat Defense デバイスの外部インターフェイスを含める必要があります。アドレスまたは FQDN をホスト エントリとしてプロファイルに追加していない場合、セッションにフィルタは適用されません。たとえば、証明書照合を作成し、証明書が基準と適切に一致した場合でも、プロファイルにデバイスをホストエントリとして追加しなければ、この証明書照合は無視されます。

セキュアクライアントのプロファイルに加えて、必要に応じて セキュアクライアント で使用できるさまざまなモジュール（AMP イネーブラなど）のプロファイルを作成できます。これらのモジュールのプロファイルをアップロードできますが、Device Manager は、セキュアクライアントプロファイルの作成のみをサポートしています。ただし、Device Manager を介して任意の種類のプロファイルをアップロードしてから、Threat Defense API を使用して（API Explorer から）、オブジェクトのプロファイルタイプを変更できます。[プロファイル（Profiles）]ページには任意のタイプのすべてのプロファイルが表示されますが、リストにはプロファイルタイプは示されません。次の手順では、これを実行する方法について説明します。

次の手順では、[オブジェクト（Objects）]ページからオブジェクトを直接作成および編集する方法を説明します。オブジェクトリストに表示される **[新規Secure Clientプロファイルの作成（Create New Secure Client Profile）]** リンクをクリックして、セキュアクライアント プロファイル オブジェクトをプロファイルプロパティの編集中に作成することもできます。

始める前に

クライアントプロファイルをアップロードするには、その前に、以下の作業を行う必要があります。

- セキュアクライアントの「Profile Editor：Windows/Standalone installer インストーラ（MSI）」をダウンロードしてインストールします。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 セキュアクライアントのバージョンです（ファイル名は変更される場合があります）。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。software.cisco.com から セキュアクライアント プロファイルエディタを入手します。このパッケージには、VPN クライアントのプロファイルエディタだけでなく、すべてのプロファイルエディタが含まれていることに注意してください。
- 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。プロファイルには、外部インターフェイスのホスト名または IP アドレスを指定する必要があります。詳細については、エディタのオンライン ヘルプを参照してください。

手順

ステップ 1 [オブジェクト（Objects）] を選択してから、目次で **[Secure Clientプロファイル（Secure Client Profiles）]** を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。
- オブジェクトに関連付けられているプロファイルをダウンロードする場合は、対象のオブジェクトの [ダウンロード（download ）] アイコン（  ）をクリックします。

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

ステップ 3 名前を入力し、オプションでオブジェクトの説明を入力します。

モジュールプロファイルをアップロードする場合は、セキュアクライアントプロファイルと区別しやすいように、モジュールタイプを示すオブジェクト名を使用してください。

ステップ 4 [アップロード（Upload）] 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 5 [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 6 [OK] をクリックしてオブジェクトを追加します。

ステップ 7 作成したプロファイルが実際にセキュアクライアントプロファイルとは異なるタイプである場合は、次の手順を実行してオブジェクトのプロファイルタイプを変更します。

a) [詳細オプション（More options）] ボタン（）をクリックし、[API エクスプローラ（API Explorer）] を選択します。

ブラウザの設定に応じて、API エクスプローラが別のタブまたはウィンドウで開きます。

b) AnyConnectClientProfile リソースを開きます。

c) GET /object/anyconnectclientprofiles メソッドを選択し、[試行する（Try It Out!）] ボタンをクリックします。

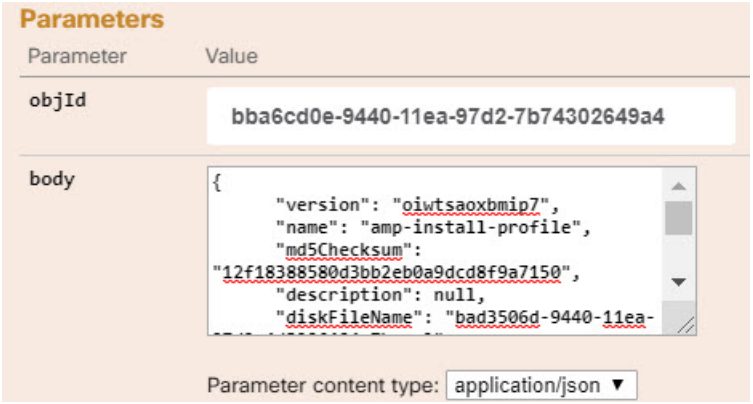
各プロファイルオブジェクトは次のように表されます。強調表示されている属性は、変更する必要がある属性です。

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile",
      "links": {
        "self": "https://10.89.5.38/api/fdm/v6/object/
anyconnectclientprofiles/bba6cd0e-9440-11ea-97d2-7b74302649a4"
      }
```

d) 出力でオブジェクトを見つけて、コードを選択し、Ctrl キーを押しながらクリックしてクリップボードにコピーします。

e) PUT /object/anyconnectclientprofiles/{objId} メソッドを選択し、その内容を [body] フィールドに貼り付けます。

f) [id] 値をコピーし、本文の上にある [objId] 編集ボックスに貼り付けます。オブジェクト ID は「自己」URL の末尾でも確認できます。



g) オブジェクトの本文にある [anyConnectModuleType] フィールドを見つけて、その値をプロファイルタイプの値に置き換えます。DART、FEEDBACK、WEB_SECURITY、ANY_CONNECT_CLIENT_PROFILE、AMP_ENABLER、NETWORK_ACCESS_MANAGER、NETWORK_VISIBILITY、START_BEFORE_LOGIN、ISE_POSTURE、UMBRELLA から選択してください。

h) 再び [body] で、[links] 属性を削除（[type] 値の後のカンマを含め）します。

オブジェクト本文は、次のようになります。

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "AMP_ENABLER",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile"
      }
```

i) [試してみる（Try It Out!）] をクリックします。応答を調べて、オブジェクトが正しく変更されたことを確認します。応答コードが 200 であり、応答本文で変更がエコーされている必要があります。GET メソッドを使用することで、結果のさらなる確認を行うことができます。

リモート アクセス VPN 経由のトラフィックの許可

リモートアクセス VPN トンネル内のトラフィックフローを有効にするには、次の方法のいずれかを使用します。

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

これは、外部ユーザがリモート アクセス VPN アドレス プール内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

このコマンドを設定するには、RA VPN 接続プロファイルで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（Bypass Access Control policy for decrypted traffic）] オプションを選択します。

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

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、リモート接続を行えることを確認します。

問題が発生した場合は、トラブルシューティング トピックに目を通し、問題の分離と修正に役立てます。リモート アクセス VPN のトラブルシューティング （37 ページ）を参照してください。

手順

ステップ 1 外部ネットワークから、セキュア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。セキュアクライアント ソフトウェアのインストール方法 （3 ページ）を参照してください。

リモートアクセス VPN 接続用のポートを変更した場合は、URL にカスタムポートを含める必要があります。たとえば、ポートを 4443 に変更した場合は、https://ravpn.example.com:4443 のような URL にします。

グループ URL を設定した場合は、それらの URL も試みてください。

ステップ 2 デバイス CLI にログインします（コマンドラインインターフェイス（CLI）へのログインを参照）。 または、CLIコンソールを開きます。

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。

統計情報では、アクティブな セキュア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 4 **show vpn-sessiondb anyconnect** コマンドを使用して、現在の VPN セッションに関する詳細情報を表示します。

詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含まれます。VPN接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  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
```

リモート アクセス VPN 設定の管理

リモートアクセス VPN 接続プロファイルは、外部ユーザーが セキュアクライアントを使用してシステムに VPN に接続することを許可するという接続特性を定義します。各プロファイルは、ユーザの認証に使用される証明書と AAA サーバ、ユーザの 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向け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 グループに可変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、複数のプロファイルを作成します。たとえば、自分の組織が異なる認証サーバを使用する別の組織と合併する場合、別の組織の認証サーバ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。

手順

ステップ 1 **[デバイス（Device）] > [リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次の[接続プロファイル]をクリックします(未選択の場合)。

ステップ 3 次のいずれかを実行します。

- 新しい接続プロファイルを作成するには、[+] ボタンをクリックします。詳細な手順については、RA VPN 接続プロファイルの設定 （19 ページ）を参照してください。
- 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。サマリー内で、[編集（Edit）] をクリックして変更できます。
- 削除ボタン（  ）をクリックすると、不要な接続プロファイルを削除できます。

- コンテンツテーブルで[グループポリシー（Group Policies）]を選択して、接続プロファイルのユーザ指向属性を定義します。「RA VPN のグループ ポリシーの設定 （29 ページ）」を参照してください。

RA VPN 接続プロファイルの設定

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

始める前に

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

- 必要な セキュアクライアント ソフトウェアパッケージを software.cisco.com からワークステーションにダウンロードします。
- リモートアクセス VPN 接続を終了する外部インターフェイスは、同じポートで HTTPS 接続を許可する管理アクセスリストを持つこともできません。管理アクセス用に別のポートを設定するか（データインターフェイスでの管理アクセス用の HTTPS ポートの設定を参照）、接続プロファイル用に別のポートを設定します。どちらのサービスもデフォルトでポート 443 を使用するため、いずれかを変更する必要があります。

手順

ステップ 1 **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次の[接続プロファイル]をクリックします(未選択の場合)。

ステップ 3 次のいずれかを実行します。

- 新しい接続プロファイルを作成するには、[+] ボタンをクリックします。
- 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。サマリー内で、[編集（Edit）] をクリックして変更できます。

ステップ 4 基本接続の属性を設定します。

- [接続プロファイル名（Connection Profile Name）]：スペースを含めずに最大 50 文字で、この接続の名前を指定します。たとえば、「MainOffice」と入力します。IP アドレスを名前として使用することはできません。

（注）
ここで入力する名前が、セキュアクライアント クライアントの接続リストに表示されます。ユーザにとってわかりやすい名前を選択してください。

- [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ユーザ名またはURLを含めることができます。VPNユーザーは、脅威に対する防御 デバイスへの接続時に、セキュアクライアント クライアントの接続リストでエイリアス名を選択できます。接続プロファイル名前は自動的にグループエイリアスとして追加されます。エイリアスは最大31文字です。

  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、セキュアクライアント 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なければなりません。グループURLはhttps://で始まる必要があります。

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

ステップ 5 プライマリ アイデンティティ ソース、および必要に応じてセカンダリ ソースを設定します。

これらのオプションにより、リモート アクセス VPN 接続を有効にするためにデバイスにユーザ認証を行う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）] には、次のアプローチを使用できます。

- [AAAのみ（AAA Only）]：ユーザ名とパスワードに基づいてユーザ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 （23 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を認証します。詳細は、接続プロファイルのための証明書認証の設定 （27 ページ）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。
- **SAML**：プライマリ認証でSAMLサーバーを使用します。SAMLを使用する場合は、フォールバックまたはセカンダリ認証ソースを設定できません。詳細については、「接続プロファイルのための AAA の設定 （23 ページ）」を参照してください。

ステップ 6 クライアントのアドレス プールを設定します。

アドレスプールは、リモートクライアントが VPN 接続を確立するときに、システムがリモートクライアントに割り当てることができる IP アドレスを定義します。詳細については、RA VPN のクライアント アドレス指定の設定 （28 ページ）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 このプロファイルに使用する [グループポリシー（Group Policy）] を選択します。

グループ ポリシーは、トンネルの確立後にユーザ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。

グループポリシーを選択すると、グループの特性の概要が表示されます。サマリー内で、[編集（Edit）] をクリックして変更できます。

必要なグループ ポリシーが存在しない場合は、ドロップダウンリストの [新しいグループポリシーの作成（Create New Group Policy）] をクリックします。

グループポリシーの詳細については、RA VPN のグループ ポリシーの設定 （29 ページ）を参照してください。

ステップ 9 [Next] をクリックします。

ステップ 10 グローバル設定を設定します。

これらのオプションは、すべての接続プロファイルに適用されます。最初の接続プロファイルを作成すると、これらのオプションは、後続の各プロファイルに対して事前に設定されます。変更すると、設定済みのすべての接続プロファイルが変更されます。

- [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。セキュアな VPN 接続を完了するには、クライアントがこの証明書を受け入れる必要があります。証明書をまだ持っていない場合、ドロップダウンリストから [内部証明書の新規作成（Create New Internal Certificate）] をクリックします。証明書を設定する必要があります。
- [外部インターフェイス（Outside Interface）]：ユーザがリモート アクセス VPN 接続を行う際の接続先インターフェイス。通常、これは外部（インターネット側）インターフェイスですが、サポートされるデバイスおよびエンドユーザ間の任意のインターフェイスを選択できます。
- [外部インターフェイス用完全修飾ドメイン名（Fully-qualified Domain Name for the Outside Interface）]：インターフェイスの名前（例：ravpn.example.com）。名前を指定すると、システムによってクラスタ プロファイルが作成されます。

  （注）
  VPN とクライアントで使用される DNS サーバが、この名前を外部インターフェイスの IP アドレスに解決できるようにする必要があります。FQDN を、該当する DNS サーバに追加します。

- [ポート（Port）]：RA VPN 接続に使用する TCP ポート。デフォルトは 443 です。RA VPN に使用されているインターフェイスで Device Manager に接続する必要がある場合は、接続プロファイルまたは Device Manager のポート番号を変更する必要があります。どちら

のサービスもデフォルトでポート 443 を使用します。リモートアクセス VPN 接続のポートを変更する場合、ユーザは URL にポート番号を含める必要があることに注意してください。

- [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：VPN トラフィックにアクセス制御ポリシーを適用するかどうか。復号された VPN トラフィックは、デフォルトでアクセス コントロールポリシーインスペクションの対象となります。[復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] を有効にすると、アクセス制御ポリシーはバイパスされますが、リモートアクセス VPN の場合、AAA サーバからダウンロードされた VPN フィルタ ACL および認証 ACL は引き続き VPN トラフィックに適用されます。

  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。また、接続プロファイル間でこのオプションの選択を変えることはできません。この機能は、すべてのプロファイルに対してオンまたはオフにします。

  このオプションを選択しない場合、外部ユーザがリモート 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。アクセス制御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、ユーザの仕様を使用してアクセスを制御することを検討してください。

  このオプションを選択することの欠点は、VPN トラフィックが検査されないことです。つまり、侵入およびファイル保護、URL フィルタリング、またはその他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

- [NAT免除（NAT Exempt）]：リモート アクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を有効にします。VPN トラフィックを NAT から除外しない場合、外部/内部インターフェイスに関する既存の NAT ルールがアドレスの RA VPN プールに適用されないようにしてください。NAT 免除ルールは、特定の送信元/宛先インターフェイスに関する手動の静的 ID の NAT ルールですが、NAT ポリシーには反映されず、隠されています。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。

  これはすべての接続プロファイルに適用されるグローバルオプションであることに注意してください。したがって、インターフェイスおよび内部ネットワークは追加するだけで、交換しないでください。そうでない場合、すでに定義済みのその他の接続プロファイルすべてに対する NAT 免除設定が変更されます。

  - [内部インターフェイス（Inside Interfaces）]：リモートユーザ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関する 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。

- **[Secure Clientパッケージ（Secure Client Package）]**：RA VPN 接続でサポートする セキュアクライアント の完全インストール ソフトウェア イメージ。パッケージごとに、ファイル名（拡張子を含む）を 60 文字以下で指定します。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。ただし、異なる接続プロファイルに対しては異なるパッケージを設定できません。別のプロファイルパッケージがすでに設定されている場合、パッケージは事前に選択されます。これを変更すると、すべてのプロファイルに対して変更されます。

  Software.cisco.com からパッケージをダウンロードします。そのエンドポイントに適合するパッケージがまだインストールされていない場合、ユーザ認証後にパッケージをダウンロードしてインストールするようユーザに促すプロンプトが表示されます。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 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。

次に、[手順（Instructions）] をクリックして、セキュアクライアント 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します。[コピー（Copy）] をクリックして、これらの指示をクリップボードにコピーし、ユーザに配布します。

ステップ 13 [Finish] をクリックします。

次のタスク

リモート アクセス VPN 経由のトラフィックの許可 （15 ページ） で説明したように、トラフィックが VPN トンネルで許可されていることを確認します。

接続プロファイルのための AAA の設定

認証、認可、およびアカウンティング（AAA） サーバは、ユーザがリモート アクセス VPN へのアクセスを許可されるかどうかを判断するためにユーザ名とパスワードを使用します。RADIUS サーバを使用する場合は、認証されたユーザ間で認証レベルを区別して、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オプション

- [ユーザ認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：リモートユーザの認証に使用されるプライマリ アイデンティティ ソース。VPN接続を完了するには、エンドユーザがこのソースか任意のフォールバック ソースで定義されている必要があります。次のいずれかを選択します。
  - Active Directory(AD)のアイデンティティレルム。必要なレルムがまだ存在していない場合は、[新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックします。
  - RADIUS サーバ グループ。
  - LocalIdentitySource (ローカルユーザデータベース): 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。
  - Duo LDAPサーバ。ただし、これは、Duo LDAP を使用した二要素認証の設定方法（50 ページ）の説明に従って二要素認証を提供するためのセカンダリ認証ソースとして使用することを推奨します。プライマリ ソースとして使用する場合、ユーザ ID 情報は取得されません。ダッシュボードにユーザ情報が表示されず、ユーザベースのアクセス コントロール ルールを作成することもできません。
  - SAML サーバ。SAML サーバを使用する場合は、フォールバックまたはセカンダリ認証ソースを設定できません。RADIUS を認可サーバとして使用できますが、認証が不要になるように RADIUS サーバを設定する必要があります。つまり、接続が SAML によって認証された後に RADIUS サーバが認可情報を提供するようにします。

- [SAMLログインエクスペリエンス（SAML Login Experience）]：プライマリ認証ソースとして SAML を選択した場合は、Web 認証を完了するために使用するクライアントブラウザを選択する必要があります。
  - [VPN クライアント組み込みブラウザ（VPN Client embedded browser）]：VPN クライアントは Web 認証に組み込みブラウザを使用するため、認証は VPN 接続にのみ適用されます。これはデフォルトであり、追加の設定は必要ありません。
  - [デフォルトOSブラウザ（Default OS Browser）]：VPN クライアントは、Web 認証にシステムのデフォルトブラウザを使用します。このオプションは、VPN認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。組み込みブラウザでは実行できない Web 認証方式（生体認証など）をサポートしたい場合も、このオプションを選択します。

    ブラウザでWeb認証を有効にするパッケージをアップロードする必要があります。パッケージは software.cisco.com から取得します。アップロードするパッケージは、デフォルトの OSブラウザで SAMLを使用するすべての接続プロファイルで使用されます。パッケージはグローバルであり、接続プロファイル固有ではありません。

- [フォールバックローカルアイデンティティソース（Fallback Local Identity Source）]：プライマリ ソースが外部サーバの場合、プライマリ サーバ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

[詳細オプション（Advanced Options）]：[詳細（Advanced）]リンクをクリックして、次のオプションを設定します。

- [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。次のオプションをイネーブルにすると、ユーザ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。
  - [ユーザ名からアイデンティティソースサーバを削除（Strip Identity Source Server from Username）]：ユーザ名を AAA サーバに渡す前に、ユーザ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が「username」として domain\username に入ると、ドメインがユーザ名から取り除かれ、認証用に 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っています。
  - [ユーザ名からグループを削除（Strip Group from Username）]：ユーザ名を AAA サーバに渡す前に、ユーザ名からグループ名を削除するかどうかを指定します。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。
- [パスワード管理を有効にする（Enable Password Management）]：パスワードの有効期限が切れたときにユーザにパスワードの変更を許可するかどうかを指定します。このオプションを選択しない場合、ユーザーのパスワードが期限切れになると、セキュアクライアントは接続を拒否するため、ユーザーは AAA サーバーにアクセスして、パスワードを変更する必要があります。このオプションを選択すると、セキュアクライアントはパスワードの有効期限が切れたときにパスワードの変更をユーザーに要求します。これは、ユーザーにとって非常に便利です。次のいずれかのオプションを選択します。また、AAA サーバで MSCHAPv2 を有効にします。
  - [パスワードの有効期限のx日前にユーザに通知（Notify user x days prior to password expiration）]（LDAP のみ）：指定した日数から始めて、パスワードの有効期限が近づいていることをユーザに警告します。1ー180 日の範囲で警告を設定できます。デフォルトは 14 です。
  - [パスワードの有効期限の日にユーザに通知（Notify user on the day of password expiration）]：ユーザに警告は表示されませんが、パスワードの有効期限が切れると、パスワードの変更を求められます。警告期間を設定している場合でも、RADIUS ユーザは常にパスワードの変更を求められます。

セカンダリアイデンティティソース

- [ユーザ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 サーバグループ、Duo LDAP サーバ、またはローカル アイデンティティ ソースを選択できます。

- [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の場合、セカンダリ サーバ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。
  - [セカンダリログインにプライマリユーザ名を使用（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。
  - [セッションサーバのユーザ名（Username for Session Server）]：認証に成功すると、ユーザ名はイベントと統計ダッシュボードに表示され、ユーザベースまたはグループベースの SSL 復号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 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 サーバのパスワードを取得する方法。このフィールドは、認証タイプに [AAAとクライアント証明書（AAA and Client Certificate）] を選択した場合にのみ適用されます。証明書オプションでは、[ユーザログインウィンドウの証明書からユーザ名を事前入力（Prefill username from certificate on user login window）] と [ログインウィンドウでユーザ名を非表示にする（Hide username in login window）] の両方を選択します。デフォルトは[プロンプト]で、ユーザにパスワードの入力を求めます。

    プライマリ サーバへのユーザ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。

    [共通パスワード]を選択してすべてのユーザに同じパスワードを使用し、[共通パスワード]フィールドにそのパスワードを入力します。

その他のオプション

- [認証サーバ（Authorization Server）]：リモート アクセス VPN ユーザを認証するように設定された RADIUS サーバ グループです。

認証が完了すると、認証によって各認証済みユーザが使用できるサービスとコマンドが制御されます。認可は、ユーザが実行を認可されていることを示す属性のセット、それらの実際の機能および制限を組み立て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に対して同じアクセスを提供します。認可のためのRADIUSの設定の詳細については、RADIUSおよびグループ ポリシーを使用したユーザの権限および属性の制御 （4 ページ）を参照してください。

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 サーバから取得した場合、RADIUS 属性は、グループ ポリシー属性をオーバーライドすることに注意してください。

- [アカウンティングサーバ（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 グループ。

  アカウンティングは、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡します。脅威に対する防御 デバイスは、RADIUS サーバにユーザアクティビティを報告します。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、デバイスを通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

接続プロファイルのための証明書認証の設定

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。証明書認証を使用している場合は、リモートアクセスユーザ接続の検証に使用する信頼できる CA 証明書に、[検証の使用（Validation Usage）] の [SSLクライアント（SSL Client）] オプションが含まれていることを確認します。

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 接続プロファイルのための AAA の設定 （23 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(組織ユニット)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名が提供され、このユーザ名がベント、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名を導出します。

- [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。
  - [ユーザログインウィンドウの証明書からユーザ名を事前入力（Prefill username from certificate on user login window）]：ユーザに認証を要求するときに、取得したユーザ名をユーザ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、ユーザ名を非表示にできます。これは、ユーザがパスワード プロンプトでユーザ名を編集できないことを意味します。

RA VPN のクライアント アドレス指定の設定

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。これらのアドレスは、AAA サーバ、DHCP サーバ、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 プールによって提供されることができます。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。

- [AAA サーバー（AAA Server）]：まず、アドレスプールのサブネットを指定する Threat Defense デバイスのネットワークオブジェクトを設定します。次に、RADIUS サーバで、オブジェクト名によりユーザの Address-Pools（217）属性を設定します。また、接続プロファイルで認証用のRADIUSサーバを指定します。
- [DHCP]：まず、1 つ以上の IPv4 アドレス範囲を持つ RA VPN の DHCP サーバを設定します（DHCP を使用して IPv6 プールを設定することはできません）。次に、DHCPサーバの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、このオブジェクトを接続プロファイルの [DHCPサーバ（DHCP Servers）] 属性で選択できます。最大10台のDHCPサーバを設定できます。

  DHCP サーバに複数のアドレス プールがある場合、[DHCP スコープ（DHCP Scope）] 属性を接続プロファイルにアタッチするグループポリシーで使用して、使用するプールを選択することができます。プールのネットワークアドレスを使用して、ホストネットワークオブジェクトを作成します。たとえば、DHCP プールに 192.168.15.0/24 および 192.168.16.0/24 が含まれている場合、DHCP スコープを 192.168.16.0 に設定すると、192.168.16.0/24 サブネットからのアドレスが必ず選択されるようになります。
- [ローカルIPアドレスプール（Local IP address pools）]：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なく、サポートするアドレス方式のみを設定します。

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。

RA VPN のグループ ポリシーの設定

グループ ポリシーは、リモート アクセス VPN 接続のための一連のユーザ指向の属性と値のペアです。接続プロファイルでは、トンネル確立後、ユーザ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、ユーザまたはユーザのグループに属性セット全体を適用できるので、ユーザ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。

手順

ステップ 1 **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次で [グループポリシー（Group Policies）] をクリックします。

ステップ 3 次のいずれかを実行します。

- [+]ボタンをクリックして、新しいエンドポイントIDグループを作成します。グループポリシーのページの属性の説明については、次のトピックを参照してください。
  - 一般属性 （30 ページ）
  - セッション設定属性 （31 ページ）
  - アドレス割り当て属性 （31 ページ）
  - スプリット トンネリング属性 （32 ページ）
  - セキュアクライアント 属性 （33 ページ）
  - トラフィック フィルタ属性 （35 ページ）
  - Windows ブラウザ プロキシ属性 （36 ページ）
- 既存のグループポリシーを編集するには、編集ボタン（）をクリックします。

- 不要なグループを削除するには、削除ボタン（）をクリックします。現在、グループを接続プロファイルで使用することはできません。

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。名前属性は唯一の必須属性です。

- [名前（Name）]：グループ ポリシーの名前。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。
- [説明（Description）]：デバイス グループの説明。説明には、最大 1,024 文字を使用できます。
- [DNSサーバ（DNS Servers）]：VPN に接続する際、クライアントがドメイン名の解決に使用する DNS サーバを定義する DNS サーバ グループを選択します。必要なグループがまだ定義されていない場合は、[DNSグループの作成（Create DNS Group）] をクリックしてすぐに作成します。
- [バナー（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。セキュアクライアントは、 部分的な HTML をサポートしています。リモート ユーザへバナーが適切に表示されることを確認するには、
タグを使用して改行を示します。
- [デフォルトドメイン（Default Domain）]：RA VPN 内のユーザ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。
- **[Secure Clientプロファイル（Secure Client Profiles）]**：[+] をクリックし、このグループに使用するセキュアクライアントプロファイルを選択します。外部インターフェイスの完全修飾ドメイン名を設定すると（接続プロファイルで）、デフォルトプロファイルが自動的に作成されます。代わりに、自分用のクライアントプロファイルをアップロードすることもできます。スタンドアロン セキュアクライアント プロファイルエディタを使用してこれらのプロファイルを作成します。スタンドアロン AnyConnect プロファイルエディタは、software.cisco.com からダウンロードしてインストールできます。クライアントプロファイルを選択しない場合、セキュアクライアントクライアントはすべてのオプションにデフォルト値を使用します。このリストの項目は、プロファイル自体ではなくセキュアクライアントプロファイル オブジェクトです。新しいプロファイルを作成（およびアップロード）するには、ドロップダウンリストで **[新規Secure Clientプロファイルの作成（Create New Secure Client Profile）]** をクリックします。

  セキュアクライアントプロファイルに加えて、AMP イネーブラなどの セキュアクライアントモジュールプロファイルを選択できます。モジュールタイプごとに1つのプロファイルを選択できます。

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）]：ログアウトして再接続することなく、ユーザがVPNに接続したままでいられる最大時間（分単位）。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]: VPN接続が自動的に閉じるまでアイドル状態である分単位の時間の長さ(1～35791394)。この連続した分数の間、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、ユーザにアラート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。
- [ユーザあたり同時ログイン（Simultaneous Logins Per User）]：ユーザ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。複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おそれがあります。

アドレス割り当て属性

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

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

  ローカルアドレスの割り当てに使用する最大6個のアドレスプールのリストを指定できます。プールの指定順序は重要です。システムでは、プールの表示順に従いそれらのプールからアドレスが割り当てられます。

- [DHCPスコープ（DHCP Scope）]：接続プロファイルのアドレス プールにDHCPサーバを設定した場合、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サブネット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、目的のプールと同じサブネット上にあり、そのプール内にはないルーティング可能なアドレスを含むネットワークオブジェクトを選択します。DHCP サーバは、このIP アドレスが属するサブネットを判別し、そのプールからのIP アドレスを割り当てます。

  ルーティングの目的で可能な場合は常に、インターフェイスのIP アドレスを使用することを推奨します。たとえば、プールが10.100.10.2 ～ 10.100.10.254 で、インターフェイス アドレスが10.100.10.1/24 の場合、DHCP スコープとして10.100.10.1 を使用します。ネットワーク番号は使用しないでください。オブジェクトがまだ存在しない場合は、[新しいネットワークの作成]をクリックします。DHCP はIPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

スプリット トンネリング属性

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

- [IPv4スプリットトンネリング（IPv4 Split Tunneling）]、[IPv6スプリットトンネリング（IPv6 Split Tunneling）]：トラフィックがIPv4 またはIPv6 アドレスを使用するかどうかによって、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オプションのいずれかを指定します。
  - [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。RA VPN 接続を行うと、ユーザのすべてのトラフィックは保護されたトンネルを通過します。これがデフォルトです。最も安全なオプションであるとも考えられます。
  - [トンネル経由で指定されたトラフィックを許可する（Allow specified traffic over the tunnel）]：宛先ネットワークとホスト アドレスを定義するネットワーク オブジェクトを選択します。これらの宛先へのトラフィックすべては、保護されたトンネルを通過します。その他のすべての宛先へのトラフィックは、クライアントによって、トンネル外の接続（ローカル Wi-Fi またはネットワーク接続など）にルーティングされます。

- [以下に指定したネットワークを除外する（Exclude networks specified below）]：宛先ネットワークまたはホストアドレスを定義するネットワークオブジェクトを選択します。これらの宛先へのトラフィックは、クライアントによって、トンネルの外の接続にルーティングされます。他の宛先へのトラフィックはトンネルを通過します。

- [スプリットDNS（Split DNS）]：クライアントが、クライアントで設定されている DNS サーバに他の 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いくつかの DNS 要求を送信するようにシステムを設定することができます。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）]：このオプションでは、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けれども、すべての DNS 要求をグループで定義された DNS サーバに保護された接続を介して送信したい場合は、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 サーバが特定のドメインのアドレスだけを解決するようにしたい場合は、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。たとえば、「example.com, example1.com」と指定します。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。

セキュアクライアント 属性

グループポリシーの セキュアクライアント 属性は、セキュア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)）]：セキュアクライアントが SSL トンネルおよび 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。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 を有効にしない場合、SSL VPN 接続を確立している セキュア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。[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。有効にする場合は、使用するデータ圧縮の方法（[圧縮（Deflate）] または [LZS（LZS）]）。[SSL圧縮（SSL Compression）] はデフォルトで無効になっています。データ圧縮は、伝送速度を上げますが、各ユーザ セッションのメモリ要件と CPU 使用率も高めます。したがって、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トしながら 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]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]オプションは、[新しいトンネル]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。この間隔は、4 ～ 10080 分（1 週間）の範囲で設定できます。

接続の設定

- [DF（フラグメント化しない）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。DF ビットが設定されているパケットの強制フラグメンテーションを許可し、それらのパケットがトンネルを通過できるようにするには、このオプションを選択します。

- [クライアントバイパスプロトコル（Client Bypass Protocol）]：セキュア ゲートウェイによる（IPv6 トラフィックだけを予期しているときの）IPv4 トラフィックの管理方法や、（IPv4 トラフィックだけを予期しているときの）IPv6 トラフィックの管理方法を設定することができます。

  セキュア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 セキュアクライアント 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に、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、クライアント プロトコル バイパス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）を設定できるようになりました。

  たとえば、セキュアゲートウェイが セキュアクライアント 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]：セキュアクライアント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バイトです。範囲は576ー1462バイトです。

- **[Secure Client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 Secure Client 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）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に適用する制限を定義します。アクセス制御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、特定のリソースを RA VPN ユーザを制限することができます。

デフォルトでは、グループ ポリシーによって RA VPN ユーザが保護されたネットワーク上の宛先へのアクセスが制限されることはありません。

- [アクセスリストのフィルタ（Access List Filter）]：拡張アクセス コントロール リスト（ACL）を使用してアクセスを制限します。スマートCLIの拡張ACLオブジェクトを選択するか、[拡張アクセスリストの作成]をクリックして作成します。

  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 TCP など）に基づいたフィルタリングが可能です。ACLはトップダウン方式で最初に一致したものから順に評価されるため、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」があります。そのため、いくつかのサブネットへのアクセスだけを拒否しながら、他のすべてのアクセスを許可したい場合は、ACL の最後に「permit any」ルールを含めるようにしてください。VPN フィルタは初期接続にのみ適用されます。アプリケーションインスペクションのアクションによって開かれたSIP メディア接続などのセカンダリ接続には適用されません。

  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、**[デバイス（Device）]**>**[詳細設定（Advanced Configuration）]**>**[スマートCLI（Smart CLI）]**>**[オブジェクト（Object）]** 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。例については、グループによって RA VPN アクセスを制御する方法 （79 ページ）を参照してください。

- [VPNをVLANに制限（Restrict Access to VLAN）]：（オプション）「VLAN マッピング」とも呼ばれます。この属性により、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 のブラウザ プロキシ属性は、ユーザ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 セッション中にブラウザプロキシ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 にブラウザ プロキシを設定するかどうかをユーザが決定できます。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 サーバ検出の使用をイネーブルにします。
- [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 サーバの IP アドレスまたはホスト名、およびプロキシ サーバ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。
  - [ブラウザ免除リスト（Browser 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。たとえば、www.example.com のポート 80 などです。リストに項目を追加するには、[追加（Add）] リンクをクリックします。項目を削除するには、ゴミ箱アイコンをクリックします。プロキシ例外リスト全体（すべてのアドレスとポートを含む）は、255 文字を超過することができません。

リモート アクセス VPN のモニタリング

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

- **show vpn-sessiondb** は VPN セッションに関する情報を表示します。これらの統計は **clear vpn-sessiondb** コマンドを使用してリセットできます。
- **show webvpn** *keyword* はリモートアクセス VPN 設定に関する情報を表示します。統計情報とインストールされている AnyConnect イメージが含まれます。**show webvpn ?** と入力し、使用可能なキーワードを確認します。

- **show aaa-server** はリモートアクセス VPN とともに使用されるディレクトリサーバに関する統計情報を表示します。

リモート アクセス VPN のトラブルシューティング

リモート アクセス VPN 接続の問題の原因は、クライアントまたは Threat Defense のデバイス設定の可能性があります。次の各項で、発生する可能性のある主な問題のトラブルシューティングについて説明します。

SSL 接続問題のトラブルシューティング

ユーザーが セキュアクライアントをダウンロードするため、外部 IP アドレスに対し セキュアクライアント を使用せずに初めて SSL 接続しようとしたが接続できない場合には、次の手順を実行します。

1. リモートアクセス VPN 接続プロファイルにデフォルト以外のポートを設定した場合は、ユーザが URL にポート番号を含めていることを確認します。たとえば、https://ravpn.example.com:4443 です。
2. クライアント ワークステーションから、外部インターフェイスの IP アドレスに ping を実行できるかどうかを確認します。実行できない場合は、ユーザのワークステーションからそのアドレスまでのルートが存在しない原因を特定します。
3. クライアント ワークステーションから、外部インターフェイスの完全修飾ドメイン名（FQDN）に ping を実行できるかどうかを確認します。この FQDN は、リモート アクセス（RA）VPN 接続プロファイルで定義されているものです。IP アドレスを ping できても、FQDN を ping できない場合は、クライアントおよび RA VPN 接続プロファイルで使用されている DNS サーバを更新し、FQDN と IP アドレスのマッピングを追加する必要があります。
4. 外部インターフェイスで提示される証明書をユーザが承認していることを確認します。ユーザはこの証明書を永久に受け入れる必要があります。
5. RA VPN 接続設定を調べ、正しい外部インターフェイスを選択していることを確認します。よくある誤りとして、RA VPN ユーザに面している外部インターフェイスではなく、内部ネットワークに面している内部インターフェイスを選択していることがあります。
6. SSL 暗号化が適切に設定されている場合は、外部スニファを使用して、TCP スリーウェイハンドシェイクが正常に実行されるかどうかを確認します。

セキュアクライアントのダウンロードおよびインストールの問題のトラブルシューティング

ユーザーが外部インターフェイスに SSL 接続可能で、セキュアクライアント パッケージをダウンロードおよびインストールできない場合、次の点を考慮してください。

- クライアントのオペレーティングシステムに対応する セキュアクライアント パッケージをアップロードしていることを確認してください。たとえば、ユーザーのワークステーションにLinuxが搭載されているのに、Linuxセキュアクライアントイメージをアップロードしなかった場合、インストールできるパッケージはありません。
- Windowsクライアントの場合、ソフトウェアのインストールには管理者権限が必要です。
- Windows クライアントの場合は、ワークステーションで ActiveX を有効にするか、または JRE 1.5 以降（JRE 7 を推奨）をインストールする必要があります。
- Safari ブラウザの場合、Java が有効であることが必要です。
- 別のブラウザを試してみてください。あるブラウザでは失敗しても、別のブラウザでは成功することがあります。

セキュアクライアント 接続問題のトラブルシューティング

外部インターフェイスに接続し、セキュアクライアントをダウンロードしてインストールできても、セキュアクライアントを使用して接続を完了できなかった場合、次のことを確認してください。

- DHCP を使用してクライアントに IP アドレスを提供しており、クライアントがアドレスを取得できない場合は、NAT ルールを確認します。RA VPN ネットワークに適用される NAT ルールには、ルート ルックアップ オプションが含まれている必要があります。ルートルックアップは、DHCP 要求が適切なインターフェイスを介して DHCP サーバーに確実に送信されるようにするために役立つ場合があります。
- 認証が失敗した場合、ユーザが正しいユーザ名とパスワードを入力しており、ユーザ名が認証サーバで正しく定義されていることを確認してください。認証サーバもデータ インターフェイスのいずれかを使用してアクセス可能である必要があります。

（注） 認証サーバが外部ネットワークにある場合は、外部ネットワークへのサイト間 VPN 接続を設定し、リモート アクセス VPN インターフェイス アドレスを VPN 内に含める必要があります。詳細については、リモート アクセス VPN を使用した外部ネットワークでのディレクトリ サーバの使用法 （63 ページ）を参照してください。

- リモートアクセス（RA）VPN 接続プロファイルで外部インターフェイスの完全修飾ドメイン名（FQDN）を設定した場合、クライアントデバイスから FQDN を ping できることを確認します。IP アドレスを ping できても、FQDN を ping できない場合、クライアントおよび RA VPN 接続プロファイルで使用されている DNS サーバを更新し、FQDN と IP アドレスのマッピングを追加する必要があります。外部インターフェイスの FQDN を指定した時に生成されたデフォルトの セキュアクライアントプロファイルを使用している場合、DNS が更新されるまでは IP アドレスを使用するようにサーバーアドレスを編集する必要があります。
- 外部インターフェイスで提示される証明書をユーザが承認していることを確認します。ユーザはこの証明書を永久に受け入れる必要があります。
- ユーザーのセキュアクライアントに複数の接続プロファイルが含まれている場合、正しいプロファイルを選択していることを確認します。
- クライアント側の設定がすべて正しいと考えられる場合は、Threat Defense デバイスに SSH 接続し、**debug webvpn** コマンドを入力します。接続試行中に表示されたメッセージを確認します。

RA VPN トラフィック フローの問題のトラブルシューティング

ユーザが安全なリモート アクセス（RA）VPN 接続を確立できても、トラフィックの送受信ができない場合は、次の操作を実行してください。

1. クライアントを切断して再接続します。これで、問題が解決することがあります。
2. セキュアクライアントで、トラフィック統計を確認して、送信カウンタと受信カウンタの両方が増えているかどうかを確認します。受信パケットカウントがゼロのままの場合、Threat Defense デバイスはトラフィックを返していません。Threat Defense の設定に問題がある可能性があります。一般的な問題を次に示します。
   - アクセスルールでトラフィックをブロックしている。アクセス制御ポリシーのルールで、ネットワーク内と RA VPN アドレス プール間のトラフィックを妨害しているルールがないかを確認します。デフォルトのアクションでトラフィックがブロックされている場合は、明示的な [許可（Allow）] ルールを作成する必要があります。
   - VPN フィルタがトラフィックをブロックしています。接続プロファイルのグループポリシーで設定されている ACL トラフィック フィルタまたは VLAN フィルタを確認します。グループポリシーに基づいてトラフィックをフィルタリングしている場合、またはその方法によっては、ACL で調整を行うか、VLAN を変更する必要があります。
   - NAT ルールが、RA VPN トラフィックでバイパスされていない。すべての内部インターフェイスの RA VPN 接続で NAT がオフに設定されていることを確認してください。または、NAT ルールが内部ネットワークとインターフェイス、および RA VPN アドレス プールと外部インターフェイス間の通信を妨害していないことを確認してください。

- ルートが誤って設定されている。すべての定義されたルートが有効で正しく機能していることを確認します。たとえば、外部インターフェイス用に定義したスタティック IP アドレスがある場合、ルーティング テーブルにデフォルト ルート（0.0.0.0/0 および ::/0）が含まれていることを確認します。
- RA VPN の DNS サーバとドメイン名が正しく設定されており、クライアント システムで正しく使用されていることを確認します。DNSサーバに到達可能であることを確認します。
- RA VPN でスプリットトンネリングが有効になっている場合、指定した内部ネットワークへのトラフィックがトンネルを通っており、他のすべてのトラフィックがトンネルをバイパスしている（Threat Defense デバイスが認識しない）ことを確認します。

3. Threat Defense デバイスに SSH 接続し、リモートアクセス VPN との間でトラフィックが送受信されていることを確認します。次のコマンドを使用します。
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

リモート アクセス VPN の例

以下に、リモート アクセス VPN を設定する例を示します。

RADIUS 認可変更の実装方法

ダイナミック認証とも呼ばれる RADIUS 認可変更（CoA）は、脅威に対する防御 リモートアクセス VPN にエンドポイントセキュリティを提供します。RA VPN の重要な課題は、侵害されたエンドポイントに対して内部ネットワークを保護し、ウイルスやマルウェアの影響を受けたときに、エンドポイントへの攻撃を修復することによって、エンドポイント自体を保護することです。エンドポイントと内部ネットワークは、RA VPN セッションの前、最中、および後のすべてのフェーズで保護する必要があります。RADIUS CoA 機能は、この目標を達成するのに役に立ちます。

Cisco Identity Services Engine (ISE) RADIUSサーバを使用する場合は、認可変更ポリシーの適用を設定できます。

ISE 認可変更機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザーまたはユーザーグループのポリシーが変更されると、ISE は CoA メッセージを 脅威に対する防御 デバイスに送信して認証を再初期化し、新しいポリシーを適用します。Inline Posture Enforcement Point（IPEP）では、脅威に対する防御 デバイスによって確立された各 VPN セッションにアクセスコントロールリスト（ACL）を適用する必要はありません。

CoA 中に変更できる属性は、リダイレクト URL、リダイレクト ACL、およびセキュリティグループタグです。

ここでは、CoA の動作とその設定方法について説明します。

認可変更へのシステム フロー

Cisco ISE には、プロセス、ファイル、レジストリエントリ、ウイルス対策保護、スパイウェア対策保護、およびホストにインストールされているファイアウォール ソフトウェアなどの条件に対するエンドポイントのコンプライアンスを評価するクライアント ポスチャ エージェントがあります。管理者はその後、エンドポイントがコンプライアンスに対応するまでネットワーク アクセスを制限したり、修復方法を確立できるようにローカル ユーザの権限を強化したりできます。ISEポスチャは、クライアント側評価を実行します。クライアントは、ISEからポスチャ要件ポリシーを受信し、ポスチャデータ収集を実行し、結果をポリシーと比較し、評価結果を ISE に返します。

次に、認可変更（CoA）処理のための 脅威に対する防御 デバイス、ISE、および RA VPN クライアントの間のシステム フローを示します。

1. リモートユーザーは、セキュアクライアントを使用して、脅威に対する防御 デバイスとの RA VPN セッションを開始します。
2. 脅威に対する防御 デバイスはそのユーザの RADIUS アクセス要求メッセージを ISE サーバに送信します。
3. クライアント ポスチャはこの時点で不明であるため、ISE は不明なポスチャに設定されている認証ポリシーにユーザを一致させます。このポリシーは、ISE が RADIUS Access-Accept の応答で 脅威に対する防御 に送信する次の cisco-av-pair オプションを定義します。
   - **url-redirect-acl=***acl_name*。ここで *acl_name* は、脅威に対する防御 デバイスで設定されている拡張 ACL の名前です。この ACL は、どのユーザ トラフィックを ISEサーバにリダイレクトすべきか（HTTP トラフィック）を定義します。例：

     ```
     url-redirect-acl=redirect
     ```

   - **url-redirect=***url*：トラフィックのリダイレクト先 URL。例：

     ```
     url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
     ```

   ホスト名を解決できるように、データインターフェイスの DNS を設定する必要があります。接続プロファイルのためにグループ ポリシーにトラフィック フィルタリングも設定する場合は、クライアント プールがポート（この例では TCP/8443）経由で ISE サーバに到達できることを確認します。
4. 脅威に対する防御 はRADIUS Accounting-Request開始パケットを送信し、ISEから応答を受信します。アカウンティング要求には、セッション ID、VPN クライアントの外部 IP アドレス、脅威に対する防御 デバイスの IP アドレスを含む、セッションの詳細がすべて含まれます。ISE はセッション ID を使用してそのセッションを識別します。脅威に対する防御 デバイスはさらに、定期的な中間アカウント情報を送信します。この情報で最も重要な属性は、脅威に対する防御 デバイスによってクライアントに割り当てられている IP アドレスを持つ Framed-IP-Address です。

5. ポスチャ状態が不明な場合、脅威に対する防御 デバイスはリダイレクト ACL に一致するクライアントからのトラフィックをリダイレクト URL にリダイレクトします。ISE は、クライアントに必要なポスチャ コンプライアンス モジュールがあるかどうかを決定し、必要に応じてユーザにインストールを指示します。
6. エージェントは、クライアントデバイスにインストールされると、ISE ポスチャポリシーで設定されたチェックを自動的に実行します。クライアントは ISE と直接通信します。クライアントは ISE にポスチャレポートを送信します。このレポートには、SWISS プロトコルおよびポート TCP/UDP 8905 を使用した複数の交換を含めることができます。
7. ISE がエージェントからポスチャレポートを受信すると、認証ルールをもう一度処理します。この時点で、ポスチャの結果が認識され、別のルールがクライアントと一致するようになります。ISE は RADIUS CoA のパケットを送信します。このパケットには準拠または非準拠のいずれかのエンドポイント向けのダウンロード可能 ACL（DACL）が含まれます。たとえば、準拠 DACL はすべてのアクセスを許可しますが、非準拠 DACL はすべてのアクセスを拒否することがあります。DACL の内容は、ISE 管理者によって設定されます。
8. 脅威に対する防御 デバイスがリダイレクションを削除します。このデバイスが DACL をキャッシュしていない場合、デバイスは ISE からダウンロードするために Access-Request を送信する必要があります。特定の DACL が VPN セッションに関連付けられますが、デバイス構成の一部にはなりません。
9. RA VPN ユーザーがもう一度 Web ページにアクセスしようとすると、ユーザーはそのセッション用に 脅威に対する防御 デバイスにインストールされている DACL によって許可されたすべてのリソースにアクセスできます。

（注） エンドポイントが必須要件を満たしていない場合、および手動修復が必要な場合は、セキュアクライアントで修復ウィンドウが開き、アクションを必要とする項目が表示されます。修復ウィンドウはバックグラウンドで実行されるため、ネットワーク アクティビティのアップデートはポップアップ表示されず、干渉や中断は発生しません。セキュアクライアントの ISE ポスチャタイル部分で [詳細（Details）] をクリックして、検出された内容およびネットワークに参加する前に必要なアップデート内容を確認できます。

Threat Defense デバイスでの認可変更の設定

認可変更ポリシーのほとんどは、ISEサーバで設定されます。ただし、脅威に対する防御 デバイスは適切に ISE に接続するように設定する必要があります。次の手順では、この構成の 脅威に対する防御 側の設定方法について説明します。

始める前に

任意のオブジェクトでホスト名を使用する場合、データおよび管理トラフィック用のDNSの設定で説明したように、データ インターフェイスと一緒に使用できるように DNS サーバが設定されていることを確認します。通常は、システムを完全に機能させるために DNS を設定する必要があります。

手順

ステップ 1 ISE への初期接続をリダイレクトするように、拡張アクセスコントロールリスト（ACL）を設定します。

リダイレクトACLの目的は、ISEがクライアントポスチャを評価できるように、初期トラフィックをISEに送信することです。ACLはISEにHTTPSトラフィックを送信しますが、ISE宛てのトラフィックや、名前解決のためにDNSサーバに送信されるトラフィックは送信しません。リダイレクト ACL の例は次のようになります。

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

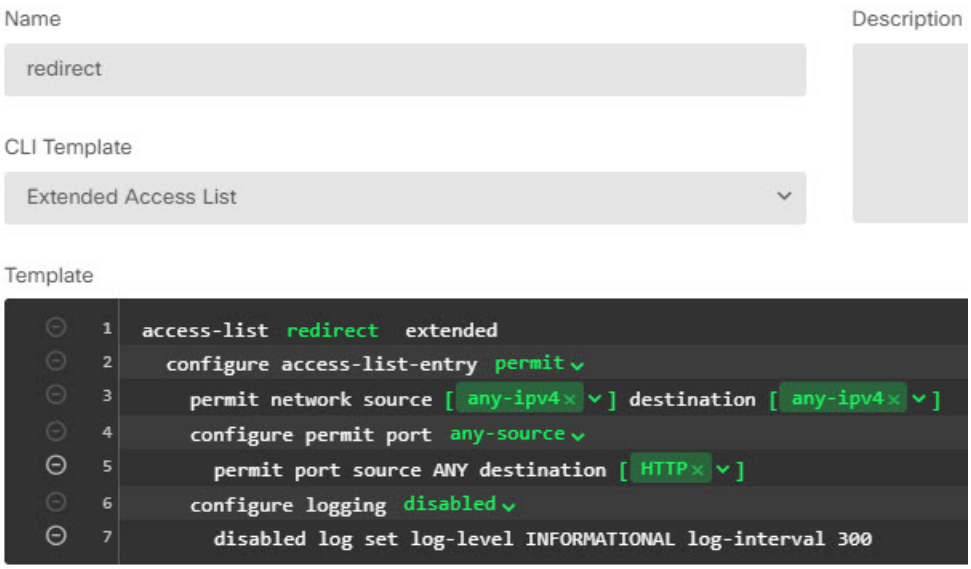
ただし、ACL には、最後のアクセス コントロール エントリ（ACE）として暗黙の「deny any any」があることに注意してください。この例では、TCP ポート www（つまりポート 80）に一致する最後の ACE は、最初の 3 つの ACE に一致するすべてのトラフィックと一致しないため、これらは冗長となります。単純に、最後の ACE を使用して ACL を作成し、同じ結果を得ることもできます。

リダイレクト ACL では、permit および deny アクションによって、ACL に一致するトラフィックが特定されることに注意してください（permit は一致、deny は不一致）。トラフィックは実際にはドロップされず、拒否されたトラフィックは ISE にリダイレクトされません。

リダイレクト ACL を作成するには、Smart CLI オブジェクトを設定する必要があります。

a) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[Smart CLI]** > **[オブジェクト（Objects）]** を選択します。
b) [+] をクリックして新しいオブジェクトを作成します。
c) ACL の名前を入力します。たとえば、**redirect** などと入力します。
d) [CLI テンプレート（CLI Template）] の場合は、[拡張アクセスリスト（Extended Access List）] を選択します。
e) [テンプレート（Template）] 本文で次のように設定します。
   - configure access-list-entry action = permit
   - source-network = any-ipv4
   - destination-network = any-ipv4
   - configure permit port = any-source
   - destination-port = HTTP
   - configure logging = disabled

ACE は次のようになります。



f) [OK]をクリックします。

この ACL は、次に変更を展開するときに設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

（注）
この ACL は IPv4 にのみ適用されます。IPv6 のサポートも追加する場合は、属性がすべて同じ 2 つ目の ACE を追加します。ただし、送信元ネットワークと宛先ネットワークには any-ipv6 を選択します。ISE または DNS サーバへのトラフィックはリダイレクトされないことを確認するために、他の ACE を追加することもできます。最初に、それらのサーバの IP アドレスを保持するホスト ネットワーク オブジェクトを作成する必要があります。

ステップ 2 RADIUS サーバ グループをダイナミック認証に設定します。

ダイナミック認証とも呼ばれる認可変更を有効にするには、RADIUS サーバとサーバ グループ オブジェクトでいくつかの重要なオプションを正確に選択する必要があります。次の手順では、これらの属性に焦点を当てています。これらのオブジェクトの詳細については、RADIUS サーバおよびグループを参照してください。

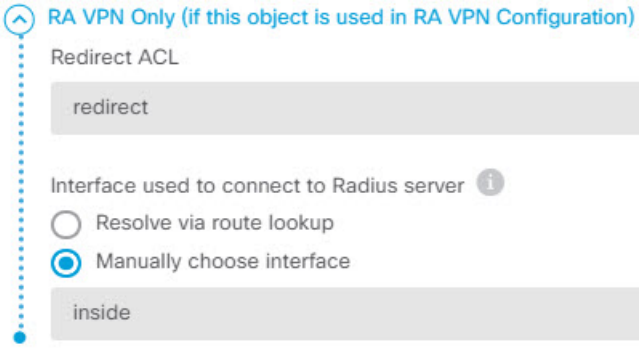
a) **[オブジェクト]** > **[アイデンティティ ソース]**を選択します。
b) **[+]** > **[RADIUSサーバ]**をクリックします。
c) サーバの名前と、ISE RADIUS サーバのホスト名または IP アドレス、認証ポート、およびサーバに設定されている秘密鍵を入力します。必要に応じてタイムアウトを調整します。これらのオプションは、ダイナミック認証には直接関連していません。
d) [RA VPN専用]リンクをクリックし、次のオプションを設定します。

- [リダイレクトACL（Redirect ACL）]：リダイレクト用に作成した拡張 ACL を選択します。この例では、redirect という名前の ACL を使用します。
- [RADIUSサーバに接続するために使用されるインターフェイス（Interface Used to Connect to RADIUS Server）]：[インターフェイスを手動で選択する（Manually Choose

Interface）] を選択し、サーバに到達できるインターフェイスを選択します。システムがインターフェイスで CoA リスナーを適切に有効化できるように、特定のインターフェイスを選択する必要があります。

Device Manager 管理アクセスにもこのサーバーを使用する場合、このインターフェイスは無視されます。管理アクセスの試行は、常に管理 IP アドレスを介して認証されます。

次の例は、内部インターフェイスに設定されているオプションを示しています。



e) [OK] をクリックしてサーバ オブジェクトを保存します。

複数の重複する ISE RADIUS サーバによる冗長設定がある場合、これらのサーバそれぞれにサーバ オブジェクトを作成します。

f) **[+]** > **[RADIUSサーバグループ]**をクリックします。

g) サーバ グループの名前を入力し、必要な場合は、デッドタイムと最大試行回数を調整します。

h) ISE サーバが別のポートを使用するように設定されている場合は、**[ダイナミック認証（Dynamic Authorization）]** オプションを選択し、ポート番号を変更します。ポート 1700 は、CoA パケットをリッスンするために使用されるデフォルトのポートです。

i) AD サーバを使用してユーザを認証するように RADIUS サーバが設定されている場合は、この RADIUS サーバと組み合わせて使用される AD サーバを指定する [RADIUS サーバをサポートするレルム（Realm that Supports the RADIUS Server）] を選択します。レルムが存在していない場合は、リストの下部にある [新しいアイデンティティ レルムの作成（Create New Identity Realm）] をクリックして作成します。

j) [RADIUSサーバ（RADIUS Server）] の下で [+] をクリックし、RA VPN 用に作成したサーバ オブジェクトを選択します。

k) [OK] をクリックしてサーバ グループ オブジェクトを保存します。

ステップ 3 **[デバイス（Device）]** > **[RA VPN]** > **[接続プロファイル（Connection Profiles）]** を選択し、この RADIUS サーバ グループを使用する接続プロファイルを作成します。

[AAA認証（AAA Authentication）] を使用し（単独または証明書と一緒に）、[ユーザ認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]、[認可（Authorization）]、および [アカウンティング（Accounting）] オプションでサーバ グループを選択します。

組織での要件に応じて、その他すべてのオプションを設定します。

（注）
DNS サーバに VPN ネットワーク経由で到達する場合、接続プロファイルで使用されるグループ ポリシーを編集し、スプリット トンネリング属性ページで [スプリットDNS（Split DNS）] オプションを設定します。

ISE での認可変更の設定

認可変更設定のほとんどは、ISEサーバで設定されます。ISEにはエンドポイントデバイス上で実行されるポスチャ アセスメント エージェントがあり、ISE はデバイスと直接通信してポスチャスタンスを決定します。脅威に対する防御 デバイスは基本的に、特定のエンド ユーザの処理に関する ISE からの指示を待ちます。

ポスチャ アセスメント ポリシーの設定の詳細は、このドキュメントの範囲外です。ただし、次の手順では、いくつかの基本について説明します。この手順をISEの設定の開始点として使用します。正確なコマンドパス、ページ名、および属性名は、リリースごとに変更される場合があることに注意してください。使用しているISEのバージョンによっては、異なる用語または構成を使用する場合があります。

サポートされる最小のISEリリースは2.2パッチ1です。

始める前に

この手順では、ISE RADIUS サーバでユーザがすでに設定済みだと仮定します。

手順

ステップ 1 **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [ネットワークデバイス（Network Devices）]** を選択し、脅威に対する防御 デバイスを ISE ネットワーク デバイス インベントリに追加して、RADIUS の設定を行います。

[RADIUS認証設定（RADIUS Authentication Settings）] を選択し、脅威に対する防御 RADIUS サーバーオブジェクトで設定されているものと同じ [共有秘密（Shared Secret）] を設定します。必要な場合は、[CoA ポート（CoA Port）] 番号を変更し、脅威に対する防御 RADIUS サーバー グループ オブジェクトで同じポートを設定していることを確認します。

ステップ 2 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能ACL（Downloadable ACLs）]** を選択します。

2つのダウンロード可能ACL (DACL)を作成します。1つは準拠エンドポイント用、もう1つは非準拠エンドポイント用です。

たとえば、非準拠エンドポイントへのすべてのアクセスを拒否(deny ip any any)し、準拠エンドポイントのすべてのアクセスを許可(deny ip any any)することができます。コンプライアンス状

態に基づいてユーザが必要とする正確なアクセスを提供するために、これらのDACLは必要なだけ複雑にすることができます。これらのDACLは認証プロファイルで使用します。

ステップ 3 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認可（Authorization）] > [認可プロファイル（Authorization Profile）]** を選択し、必要なプロファイルを設定します。

次の状態のプロファイルが必要です。それぞれの最小属性が表示されます。

- [不明（Unknown）]：不明なポスチャ プロファイルはデフォルトのポスチャ プロファイルです。すべてのエンドポイントは、RA VPN 接続の最初の確立時にこのポリシーに一致します。このルールのポイントは、リダイレクト ACL と URL を適用し、ポスチャエージェントがエンドポイント上に存在していない場合は、これをダウンロードすることです。エンドポイントは、エージェントがインストールされていない場合、またはインストールが失敗した場合、このプロファイルが適用されたままとなります。そうでない場合、エンドポイントはポスチャを評価した後に準拠または非準拠プロファイルに移行します。

  最小属性は次のとおりです。

  - [名前（Name）]：PRE_POSTURE など。
  - [アクセスタイプ（Access Type）]：[ACCESS_ACCEPT] を選択します。
  - [共通タスク（Common Tasks）]：[Webリダイレクション（CWA、DRW、MDM、NSP、CPP）（Web Redirection (CWA, DRW, MDM, NSP, CPP)）] を選択し、次に [クライアント プロビジョニング（ポスチャ）（Client Provisioning (Posture)）] を選択し、脅威に対する防御 デバイスで設定したリダイレクト ACL の名前を入力します。[値（Value）] では、[クライアントプロビジョニング ポータル（Client Provisioning Portal）] を選択します（まだ選択していない場合）。
  - [属性の詳細（Attribute Details）] には、url-redirect-acl および url-redirect の 2 つの cisco-av-pair 値が表示されている必要があります。ISE はこのデータを 脅威に対する防御 デバイスに送信し、RA VPN ユーザ セッションに条件が適用されます。

- [準拠（Compliant）]：ポスチャ アセスメントが完了した後、エンドポイントに設定されたすべての要件を満たしている場合、クライアントは準拠と見なされてこのプロファイルを取得します。通常、このクライアントにはフルアクセスを付与します。

  最小属性は次のとおりです。

  - [名前（Name）]：FULL_ACCESS など。
  - [アクセスタイプ（Access Type）]：[ACCESS_ACCEPT] を選択します。
  - [共通タスク（Common Tasks）]：[DACL名（DACL Name）] を選択し、準拠ユーザ向けにPERMIT_ALL_TRAFFIC などのダウンロード可能ACL を選択します。ISE はACL を 脅威に対する防御 デバイスに送信し、デバイスが ACL をユーザ セッションに適用します。この DACL は、ユーザ セッションの最初のリダイレクト ACL を置き換えます。

- [非準拠（Non-compliant）]：ポスチャ アセスメントによってエンドポイントがすべての要件を満たしていないことが決定された場合、必要な更新プログラムをインストールするなどにより、クライアントがエンドポイントを準拠させることができるカウントダウンが存在します。セキュアクライアントは、準拠の問題をユーザーに通知します。カウントダウンの間、エンドポイントは不明な準拠状態になります。カウントダウンの期限が切れてもエンドポイントが非準拠のままである場合、セッションは非準拠としてマークされ、非準拠プロファイルが取得されます。通常、このエンドポイントに対するすべてのアクセスを禁止するか、少なくとも何らかの方法でアクセスを制限します。

  最小属性は次のとおりです。

  - [名前（Name）]：Non_Compliant など。
  - [アクセスタイプ（Access Type）]：[ACCESS_ACCEPT] を選択します。
  - [共通タスク]: [DACL名]を選択し、非準拠ユーザ向けにDENY_ALL_TRAFFICなどのダウンロード可能ACLを選択します。ISE は ACL を 脅威に対する防御 デバイスに送信し、デバイスが ACL をユーザ セッションに適用します。この DACL は、ユーザ セッションの最初のリダイレクト ACL を置き換えます。

ステップ 4 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択し、次のリソースを設定します。

- [AnyConnectパッケージ（AnyConnect package）]：software.cisco.com からダウンロードしたヘッドエンドパッケージ ファイル。サポートするクライアント プラットフォームごとに別個のパッケージが必要です。そのため、AnyConnectDesktopWindows などの複数のタイプを設定する必要があります。
- [ISEポスチャ設定ファイル（タイプ：AnyConnectProfile）（ISE Posture Configuration File (Type: AnyConnectProfile)]：この設定ファイルは、コンプライアンス モジュールがエンドユーザのデバイスを評価するために使用する設定を定義します。このファイルはまた、ユーザが非準拠デバイスを準拠させるために使用できる時間の長さを定義します。
- [コンプライアンス モジュール パッケージ（タイプ：ComplianceModule）（Compliance Module Package (Type: ComplianceModule)）]：セキュアクライアント コンプライアンス モジュール ファイルは、エンドポイントのコンプライアンスを確認するためにインストールされた AnyConnect パッケージにプッシュされるファイルです。[Ciscoサイトからリソースを追加（Add Resource from Cisco Site）] コマンドを使用してこのファイルをダウンロードします。設定した セキュアクライアント パッケージに基づいた正しいモジュールをダウンロードしてください。そうしないと、ユーザーはダウンロードに失敗します。software.cisco.com で、ISEComplianceModule フォルダ内の セキュアクライアント リストでこれらのファイルを検索することもできます。
- [AnyConnect設定ファイル（タイプ：AnyConnectConfig）（AnyConnect Configuration File (Type: AnyConnectConfig)）]：これらの セキュアクライアント リリース固有設定は、[AnyConnectパッケージ（AnyConnect Package）]、[コンプライアンスモジュール（Compliance Module）]、および適用する [ISEポスチャ（ISE Posture）] を定義します。パッケージは OS

固有であるため、サポートするクライアントOS（Windows、MAC、Linuxなど）ごとに個別の設定ファイルを作成します。

ステップ5 **[ポリシー]** > **[クライアントプロビジョニング]**を選択し、クライアントプロビジョニングポリシーを設定します。

CoA を実装する必要があるオペレーティングシステムごとに、CoA_ClientProvisionWin などの名前を持つ新しいルールを作成します。ルールに適したオペレーティングシステムを選択し、[結果（Results）] で、OS 用に作成した セキュアクライアント 設定ファイルを [エージェント（Agent）] として選択します。

置換するデフォルトのOS固有のルールを無効にします。

ステップ6 ポスチャポリシーを設定します。

この手順では、組織に適したポスチャ要件を作成します。

- **[ポリシー]** > **[ポリシー要素]** > **[条件]** > **[ポスチャ]**を選択し、満たす必要がある単純なポスチャ条件を定義します。たとえば、ユーザに特定のアプリケーションのインストールを要求する場合があります。
- **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]** > **[要件（Requirements）]** を選択し、エンドポイントのコンプライアンスモジュール要件を定義します。
- **[ポリシー（Policy）]** > **[ポスチャ（Posture）]** > **[ポスチャポリシー（Posture Policy）]** を選択し、サポートされるオペレーティングシステムのポリシーを設定します。

ステップ7 **[ポリシー]** > **[ポリシーセット]** > **[デフォルト]** > **[認証ポリシー]**を選択し、ポリシーを作成します。

準拠条件ごとにルールを追加します。次のサンプル値は、前の手順の例に基づいています。

- [不明（Unknown）] : pre-posture およびポスチャ ダウンロード用。
  - [名前（Name）] : PRE_POSTURE など
  - [条件（Conditions）] : ”Session-PostureStatus EQUALS Unknown” および “Radius-NAS-Port-Type EQUALS Virtual”。
  - [プロファイル（Profiles）] : PRE_POSTURE など。
- [準拠（Compliant）] : ポスチャ要件を満たすクライアント用。
  - [名前（Name）] : FULL_ACCESS など
  - [条件（Conditions）] : ”Session-PostureStatus EQUALS Compliant” および “Radius-NAS-Port-Type EQUALS Virtual”。
  - [プロファイル（Profiles）] : FULL_ACCESS など
- [非準拠（Non-compliance）] : ポスチャ要件を満たさないクライアント用。

- [名前（Name）]：Non_Compliant など。
- [条件（Conditions）]：”Session-PostureStatus EQUALS NonCompliant” および “Radius-NAS-Port-Type EQUALS Virtual”。
- [プロファイル（Profiles）]：Non_Compliant など

ステップ 8 （オプション）。**[管理]** > **[設定]** > **[ポスチャ]** > **[再評価]**を選択し、ポスチャ再評価を有効にします。

デフォルトでは、ポスチャは接続時にのみ評価されます。ポスチャ再評価をイネーブルにして、接続されたエンドポイントのポスチャを定期的に確認できます。再評価間隔を設定して、発生頻度を決定できます。

システムが再評価に失敗した場合は、システムの応答方法を定義できます。ユーザの続行を許可する（接続したまま）、ユーザをログオフさせる、またはユーザにシステムの修復を依頼することができます。

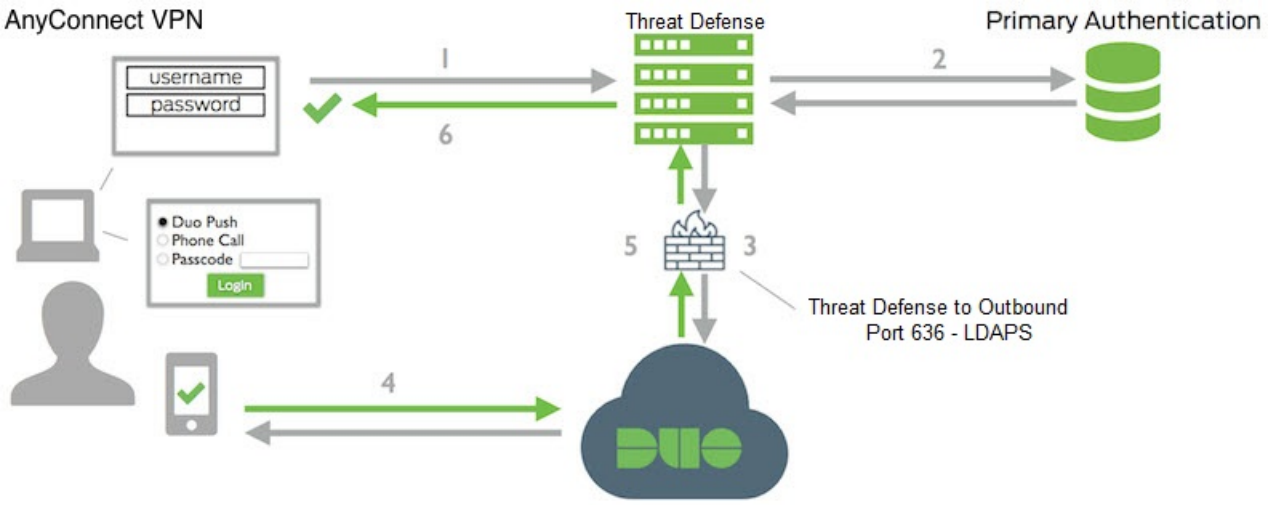
Duo LDAP を使用した二要素認証の設定方法

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

以降のトピックでは設定についてさらに詳しく説明します。

Duo LDAP セカンダリ認証のシステム フロー

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



次に、システムフローについて説明します。

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

Duo LDAP セカンダリ認証の設定

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

手順

ステップ 1 Duoアカウントを作成し、統合キー、秘密キー、およびAPIホスト名を取得します。

次に、プロセスの概要を示します。詳細については、Duo の Web サイト（https://duo.com）を参照してください。

a) Duo アカウントへのサインアップ
b) Duo Admin Panel にログインし、[アプリケーション（Applications）] に移動します。
c) [アプリケーションの保護（Protect An Application）] をクリックし、アプリケーションリストで Cisco SSL VPN を探します。[アプリケーションの保護（Protect this Application）] をクリックし、統合キー、秘密キー、および API ホスト名を取得します。詳細については、Duo の『*Getting Started*』ガイド（https://duo.com/docs/getting-started）を参照してください。

ステップ 2 Duo LDAP サーバの Duo LDAP アイデンティティソースを作成します。

Duo LDAP オブジェクトを作成するには、脅威に対する防御 API を使用する必要があります。Device Manager を使用して作成することはできません。API Explorerを使用するか、独自のクライアントアプリケーションを作成してオブジェクトを作成できます。次の手順では、API Explorerを使用してオブジェクトを作成する方法について説明します。

a) Device Manager にログインし、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

ブラウザの設定に応じて、API エクスプローラが別のタブまたはウィンドウで開きます。

b) （オプション）。Duo LDAPサーバに接続するためにシステムが使用するインターフェイスの特定に必要な値を取得します。

インターフェイスを指定しない場合は、ルーティングテーブルが使用されます。必要に応じて、Duo LDAP サーバのスタティックルートを作成できます。または、Duo LDAPオブジェクトで使用するインターフェイスを指定できます。インターフェイスを指定する場合は、インターフェイスグループのさまざまなGETメソッドを使用して、必要な値を取得します。物理インターフェイス、サブインターフェイス、EtherChannel、またはVLANインターフェイスを使用できます。たとえば、物理インターフェイスの値を取得するには、GET /devices/default/interfacesメソッドを使用して、使用する必要があるインターフェイスのオブジェクトを検索します。インターフェイスオブジェクトから次の値が必要です。

- ID
- タイプ
- バージョン
- 名前

c) [DuoLDAPIdentitySource] 見出しをクリックして、グループを開きます。
d) [POST /object/duoldapidentitysources] メソッドをクリックします。
e) [パラメータ（Parameters）] 見出しの [本文（body）] 要素について、右側の [データタイプ（Data Type）] 列の [サンプル値表示（Example Value display）] ボックスをクリックします。このアクションにより、本文の値の編集ボックスに例がロードされます。
f) [本文の値（body value）] 編集ボックスで、次の手順を実行します。

- 属性行の **version**、**id** を削除します（これらの属性は、PUT 呼び出しには必要ですが POST には必要ありません）。
- [名前]には、Duo-LDAP-serverなどのオブジェクトの名前を入力します。
- [説明]では、参照用にオブジェクトのわかりやすい説明を入力するか、属性行を削除します。
- [apiHostname]には、Duoアカウントから取得したAPIホスト名を入力します。ホスト名は API-XXXXXXXX.DUOSECURITY.COM のような形式になります。X の部分を一意の値に置き換えます。大文字は必須ではありません。
- [ポート]には、LDAPSに使用するTCPポートを入力します。Duoから別のポートを使用するように指示されていない限り、これは636になります。アクセス制御リストで、必ずこのポートを介した Duo LDAP サーバへのトラフィックを許可してください。
- [タイムアウト]には、Duoサーバに接続する際のタイムアウトを秒単位で入力します。値は1ー300秒です。デフォルトは 120 です。デフォルトを使用するには、120を入力するか、属性行を削除します。

- [IntegrationKey]には、Duoアカウントから取得した統合キーを入力します。
- [secretKey]には、Duoアカウントから取得した秘密キーを入力します。このキーはその後マスクされます。
- [インターフェイス]には、Duo LDAPサーバに接続するために使用するインターフェイスのID、タイプ、バージョン、および名前の値を入力するか、インターフェイス属性を定義するために使用する6つの行を削除します(末尾の閉じ括弧を含む)。
- [タイプ]では、値はduoldapidentitysourceのままにします。

たとえば、オブジェクトの本文は次のようになります。apiHostname と integrationKey は不明瞭にしてありますが、秘密キーは意図的に仮のものを示しています。

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXX.DUOSECURITY.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

g) [試してみる（Try It Out!）] ボタンをクリックします。

システムは、curlコマンドを発行してオブジェクトをデバイス設定にポストします。curlコマンド、応答本文、および応答コードが表示されます。有効な本文を作成した場合は、[応答コード（Response Code）] フィールドに **200** と表示されます。

エラーが発生した場合は、応答本文でエラーメッセージを確認します。本文の値を修正して再試行できます。

h) トップメニューで [デバイス（Device）] をクリックして、Device Manager に戻ります。

i) [オブジェクト]を選択し、目次から[アイデンティティソース]を選択します。

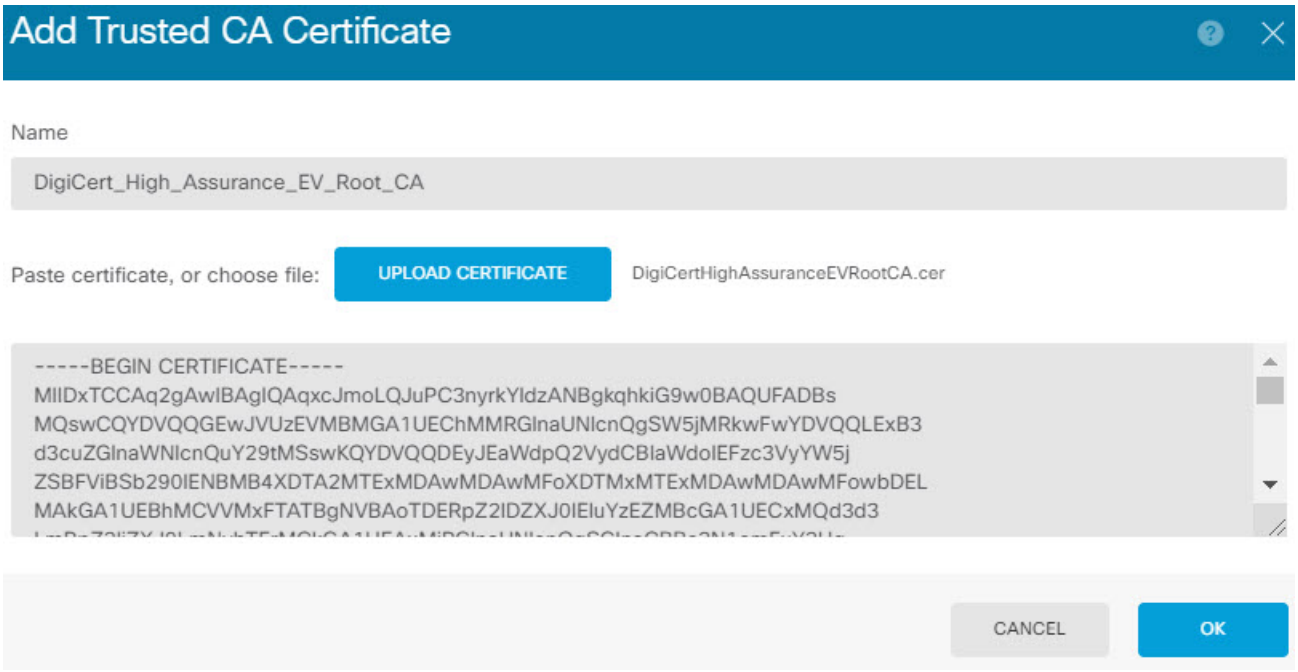
Duo LDAPオブジェクトがリストに表示されます。表示されない場合は、API Explorerに戻り、オブジェクトの作成を再試行します。GETメソッドを使用して、実際に作成されたかどうかを確認できます。

Device Manager を使用してオブジェクトを削除できますが、編集したりその内容を表示したりすることはできません。これらの操作にはAPIを使用する必要があります。関連するメソッドは [DuoLDAPIdentitySource] グループに表示されます。

ステップ 3 Duo Web サイトの信頼できる CA 証明書を Device Manager にアップロードします。

Threat Defense システムには、Duo LDAP サーバーへの接続を検証するために必要な証明書がなければなりません。Google Chromeブラウザで実行する次の手順を使用して、証明書を取得してアップロードできます。ご使用のブラウザの手順は異なる場合があります。または、https://www.digicert.com/digicert-root-certificates.htmに直接移動して証明書をダウンロードすることもできますが、次の手順は一般的なものであり、任意のサイトの信頼できるルートCA証明書を取得するために使用できます。

a) ブラウザでhttps://duo.comを開きます。
b) ブラウザの URL フィールドでサイト情報リンクをクリックし、[証明書（Certificate）] リンクをクリックします。この操作により、証明書情報ダイアログボックスが開きます。
c) [証明のパス（Certificate path）] タブをクリックし、パスのルート（最上位）を選択します。この場合はDigiCertです。
d) DigiCert を選択した状態で、[証明書の表示（View Certificate）] をクリックします。この操作により、新しい証明書ダイアログボックスが開き、[一般]タブにDigiCert High Assurance EV Root CAに対して証明書が発行されたことが示されます。これは、Device Manager にアップロードする必要があるルート CA 証明書です。
e) [詳細（Details）] タブをクリックし、[ファイルにコピー（Copy to File）] ボタンをクリックして、証明書のダウンロードウィザードを起動します。
f) ウィザードを使用して、ワークステーションに証明書をダウンロードします。デフォルトのDER形式を使用してダウンロードします。
g) Device Manager で、**[オブジェクト（Objects）] > [証明書（Certificates）]** を選択します。
h) **[+] > [信頼済みCAの証明書の追加（Add Trusted CA Certificate）]** をクリックします。
i) 証明書の名前を入力します(例: DigiCert_High_Assurance_EV_Root_CA) (スペースは使用できません)。
j) [証明書のアップロード（Upload Certificate）] をクリックし、ダウンロードしたファイルを選択します。



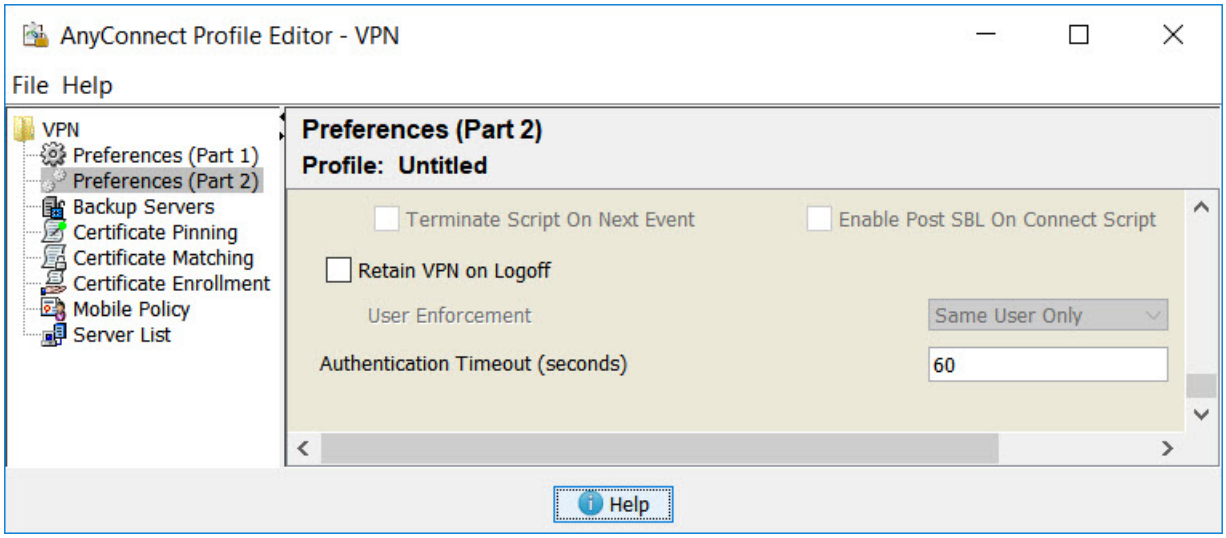
k) [OK]をクリックします。

ステップ 4 セキュアクライアント プロファイルエディタを使用して、認証タイムアウトに 60 秒以上を指定するプロファイルを作成します。

ユーザがDuoのパスコードを取得し、セカンダリ認証を完了するために、余裕を持った時間を指定する必要があります。60秒以上を推奨します。

セキュアクライアント プロファイルの作成とアップロードの詳細については、クライアント プロファイルの設定およびアップロード （12 ページ）を参照してください。次の手順では、認証タイムアウトのみを設定してから、Threat Defense にプロファイルをアップロードする方法について説明します。他の設定を変更する場合は、ここで行ってください。

a) セキュアクライアント プロファイル エディタ パッケージをダウンロードしてインストールします（まだ行っていない場合）。このパッケージは、Cisco Software Center（software.cisco.com）の使用しているセキュアクライアントバージョンのフォルダにあります。
b) セキュアクライアント の **VPN プロファイルエディタ**を開きます。
c) 目次の [設定（パート2）（Preferences (Part 2)）] を選択し、ページの最後までスクロールして、[認証タイムアウト（Authentication Timeout）] を 60 以上に変更します。次の図は AnyConnect 4.7 VPN プロファイルエディタからの引用です。それより前のバージョンや後のバージョンでは、内容が異なる場合があります。



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

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

e) Device Manager で、**[オブジェクト（Objects）] > [Secure Clientプロファイル（Secure Client Profiles）]** を選択します。
f) [+] をクリックして新しいプロファイルオブジェクトを作成します。
g) [名前（Name）]に、オブジェクトの名前を入力します。たとえば、Duo-LDAP-profile と入力します。
h) [アップロード（Upload）] をクリックし、作成した XML ファイルを選択します。
i) [OK]をクリックします。

ステップ 5 グループポリシーを作成し、ポリシーで セキュアクライアント プロファイルを選択します。

ユーザに割り当てるグループポリシーは、接続のさまざまな側面を制御します。次の手順では、プロファイルXMLファイルをグループに割り当てる方法について説明します。グループポ

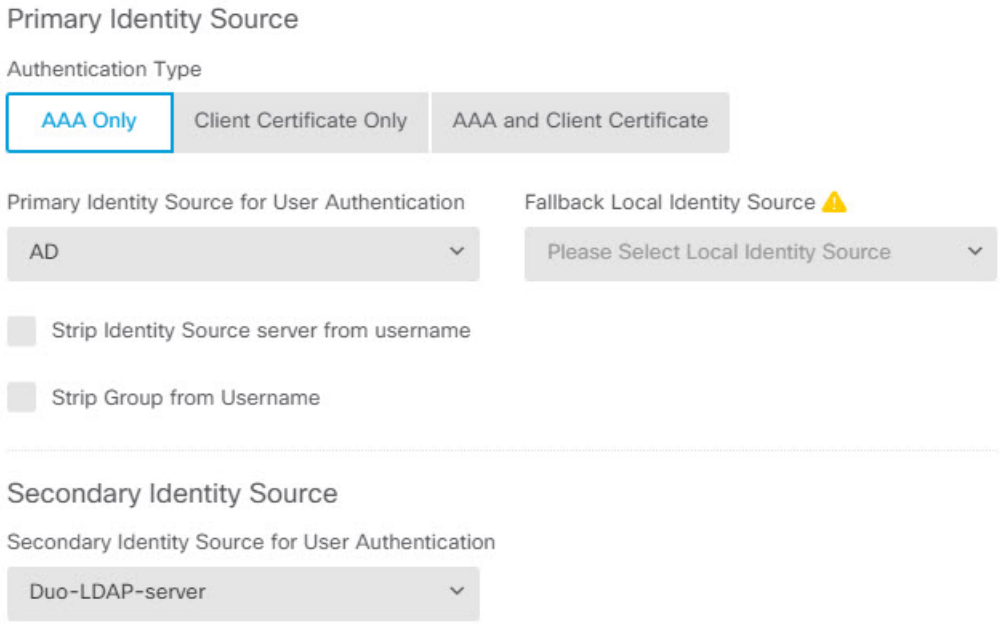
リシーで実行できる操作の詳細については、RA VPN のグループ ポリシーの設定 （29 ページ） を参照してください。

a) **[デバイス（Device）] > [リモートアクセスVPN（Remote Access VPN）]** で [設定の表示（View Configuration）] をクリックします。
b) 目次で[グループポリシー]をクリックします。
c) DfltGrpPolicy を編集するか、[+] をクリックして新しいグループポリシーを作成します。たとえば、すべてのユーザに対して 1 つのリモートアクセス VPN 接続プロファイルが必要な場合は、デフォルトのグループポリシーを編集することが適切です。
d) [全般]ページで、次のプロパティを設定します。
   - [名前]: 新しいプロファイルの場合は、名前を入力します。たとえば、Duo-LDAP-group と入力します。
   - **[Secure Clientプロファイル（Secure Client Profiles）]** : [+] をクリックし、作成したセキュアクライアント プロファイルを選択します。
e) [OK] をクリックしてグループプロファイルを保存します。

ステップ 6 Duo LDAP セカンダリ認証に使用するリモートアクセス VPN 接続プロファイルを作成または編集します。

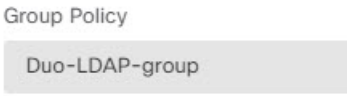
接続プロファイルを設定するには数多くの手順があります。詳細については、RA VPN 接続プロファイルの設定 （19 ページ） を参照してください。次の手順では、Duo-LDAP をセカンダリ認証ソースとして有効にし、セキュアクライアントクライアントプロファイルを適用するための主な変更について説明します。新しい接続プロファイルの場合は、残りの必須フィールドも設定する必要があります。この手順では、既存の接続プロファイルを編集しており、これら2つの設定だけ変更する必要があると仮定しています。

a) [RA VPN]ページで、目次の[接続プロファイル]をクリックします。
b) 既存の接続プロファイルを編集するか、新規に作成します。
c) [プライマリアイデンティティソース]で、次を設定します。
   - [認証タイプ（Authentication Type）] : [AAAのみ（AAA Only）] または [AAAとクライアント証明書（AAA and Client Certificate）] のいずれかを選択します。AAAを使用していない場合、二要素認証を設定できません。
   - [ユーザ認証のプライマリアイデンティティソース]: プライマリActive DirectoryまたはRADIUSサーバを選択します。プライマリソースとしてDuo-LDAPアイデンティティソースを選択できることに注意してください。ただし、Duo-LDAP は認証サービスのみを提供し、アイデンティティサービスは提供しないため、プライマリ認証ソースとして Duo-LDAP を使用する場合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザ名は表示されず、これらのユーザに対してアクセス コントロール ルールを作成することはできません(必要に応じて、ローカルアイデンティティソースへのフォールバックを設定できます)。
   - [セカンダリアイデンティティソース（Secondary Identity Source）] : Duo-LDAP のアイデンティティソースを選択します。



d) [Next] をクリックします。

e) [リモートユーザ（Remote User）]ページで、作成または編集した[グループポリシー（Group Policy）] を選択します。



f) このページの [次へ（Next）] をクリックし、次のページの [グローバル設定（Global Settings）] をクリックします。

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

ステップ 7 変更を保存します。

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

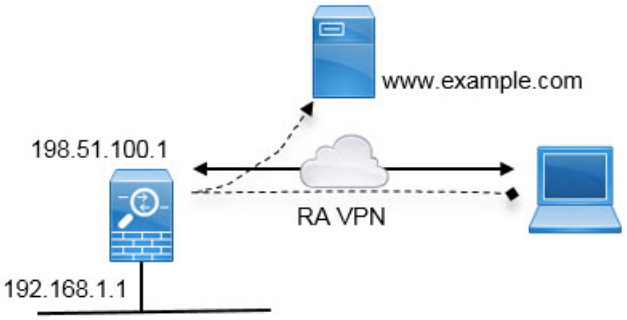
b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

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

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

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

次の図は、例を示しています。外部インターフェイス、198.51.100.1 に設定されているリモート アクセス VPN があります。リモート ユーザの VPN トンネルを分割し、インターネットに向かうトラフィックを外部インターフェイスから戻し、内部ネットワークに向かうトラフィックはデバイスを通過し続けるようにできます。そのため、リモートユーザがインターネット上のサーバ（www.example.com など）にアクセスする場合、接続は最初に VPN を通過し、その後 198.51.100.1 インターフェイスからインターネットにルートバックされます。



次の手順では、このサービスの設定方法について説明します。

始める前に

この例は、デバイスが登録済み、リモートアクセス VPN ライセンスが適用済み、セキュアクライアントイメージがアップロード済みであることを前提としています。アイデンティティポリシーでも使用されるアイデンティティ レルムも設定済みであると想定しています。

手順

ステップ 1 リモートアクセス VPN 接続を設定します。

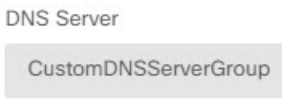
設定には、接続プロファイルだけでなく、カスタマイズされたグループポリシーが必要です。ヘアピニングは一般的な設定であり、グループポリシーで必要な設定がほぼ該当するため、この例では新しいグループポリシーを作成するのではなく、デフォルトグループポリシーを編集します。どちらのアプローチも取ることができます。

a) **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。

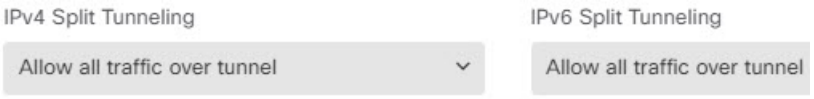
b) 目次の [グループポリシー（Group Policies）] をクリックし、DfltGrpPolicy オブジェクトの編集アイコン（）をクリックします。

c) デフォルトグループポリシーに次の変更を加えます。

- [全般（General）] ページの [DNSサーバ（DNS Server）] で、VPN エンドポイントがドメイン名を解決するために使用する必要がるサーバを定義する DNS サーバ グループを選択します。



- [スプリットトンネリング（Split Tunneling）] ページで、**IPv4** と IPv6 の両方の**スプリットトンネリング**で [すべてのトラフィックをトンネル経由で許可（Allow all traffic on tunnel）] オプションを選択します。これはデフォルト設定であるため、すでに正しく設定されている可能性があります。



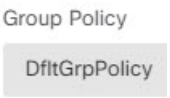
（注）
これは、ヘアピン接続を有効にするための重要な設定です。すべてのトラフィックを VPN ゲートウェイに向かわせる場合、スプリット トンネリングは、リモート クライアントが VPN の外部にあるローカル サイトやインターネット サイトに直接アクセスできるようにするための方法です。

d) [OK] をクリックして、デフォルトグループポリシーの変更を保存します。

e) [接続プロファイル（Connection Profiles）] をクリックし、既存のプロファイルを編集するか、または新しいプロファイルを作成します。

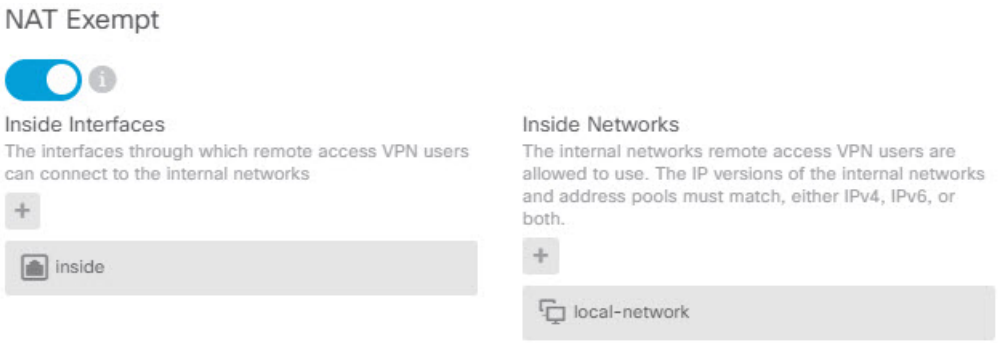
f) 接続プロファイルで、ウィザードのページを表示し、他の RA VPN 設定の場合と同じようにすべてのオプションを設定します。ただし、ヘアピン接続を有効にするには、次のオプションを正しく設定する必要があります。

- 手順 2 の [グループポリシー（Group Policy）]。ヘアピニング用にカスタマイズしたグループポリシーを選択します。



- 手順 3 の [NAT免除（NAT Exempt）]。この機能を有効にします。内部インターフェイスを選択し、内部ネットワークを定義するネットワーク オブジェクトを選択します。この例では、オブジェクトは 192.168.1.0/24 を指定します。内部ネットワークに向かう RA VPN トラフィックは、アドレス変換されません。ただし、ヘア ピニングされたトラフィックは外部インターフェイスの外に出るため、引き続き NAT が行われます。これは、NAT 免除は内部インターフェイスにのみ適用されるためです。他に定義済み

の接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。



（注）
[NAT免除（NAT Exempt）] オプションは、ヘアピン設定のもう 1 つの重要な設定です。

g) （オプション）。[グローバル設定]で、[復号されたトラフィックでアクセス コントロール ポリシーをバイパスする(sysopt permit-vpn)]オプションを選択します。

このオプションを選択すると、RA VPN プールアドレスからのトラフィックを許可するアクセス制御ルールを設定する必要がなくなります。このオプションはセキュリティを向上（外部ユーザがプール内のアドレスをスプーフィングできません）させますが、RA VPN トラフィックが、URL フィルタリングや侵入防御を含むインスペクションから除外されることを意味します。このオプションを決定する前に、長所と短所を考慮してください。

h) RA VPN の設定を確認してから [完了（Finish）] をクリックします。

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

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

次の手順で、必要なルールを作成する方法を説明します。

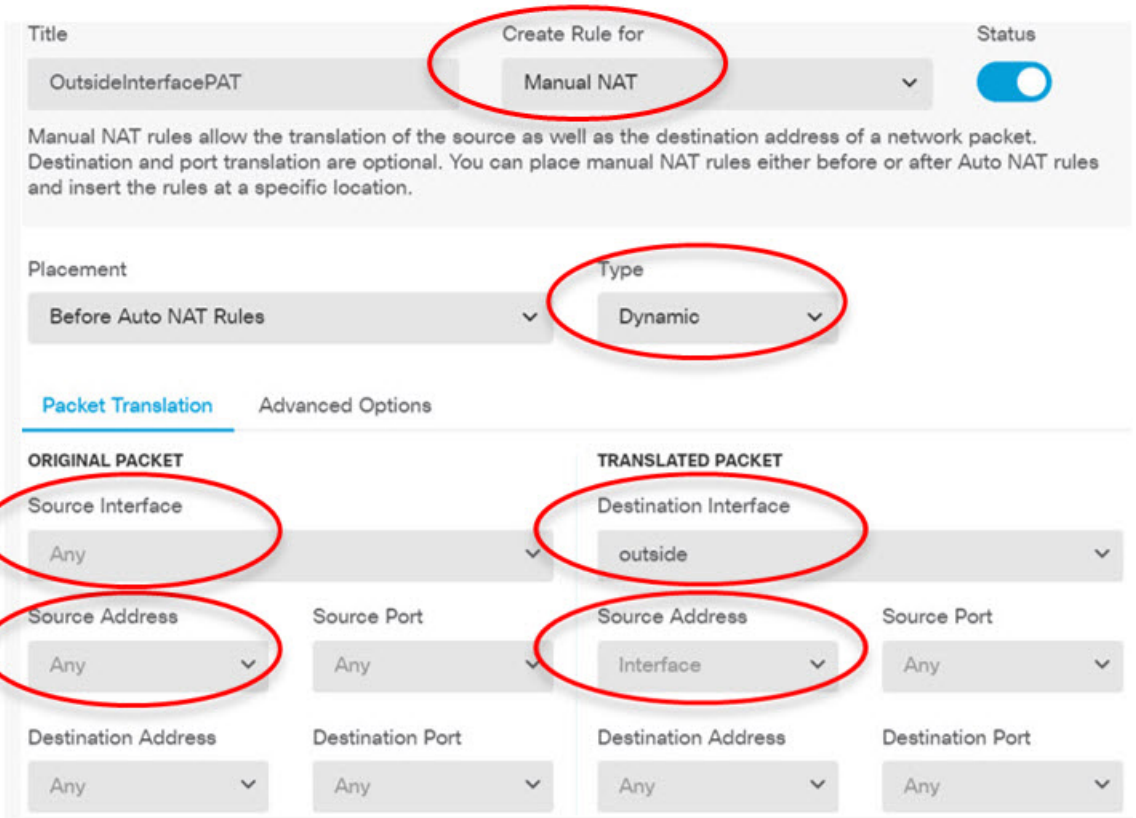
a) **[ポリシー（Policies）] > [NAT]** をクリックします。
b) 次のいずれかを実行します。

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

c) 次のプロパティを指定してルールを設定します。

- [タイトル（Title）]：新しいルールの場合は、スペースを含めずにわかりやすい名前を入力します。例、OutsideInterfacePAT。
- [ルールの作成対象（Create Rule For）]：[手動 NAT（Manual NAT）]。
- [配置（Placement）]：[自動 NAT ルールの前（Before Auto NAT Rules）]（デフォルト）。
- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [元のパケット（Original Packet）]：[送信元アドレス（Source Address）] の場合は、[任意（Any）] または any-ipv4 を選択します。[送信元インターフェイス（Source Interface）] の場合は、デフォルトの [任意（Any）] を必ず選択してください。[元のパケット（Original Packet）] のその他すべてのオプションは、デフォルトの [任意（Any）] のままにします。
- [Translated Packet（変換後のパケット）]：[宛先インターフェイス（Destination Interface）] の場合は、[外部（outside）] を選択します。[変換後のアドレス（Translated Address）] の場合は、[インターフェイス（Interface）] を選択します。[Translated Packet（変換後のパケット）] のその他すべてのオプションは、デフォルトの [任意（Any）] のままにします。

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



d) [OK] をクリックします。

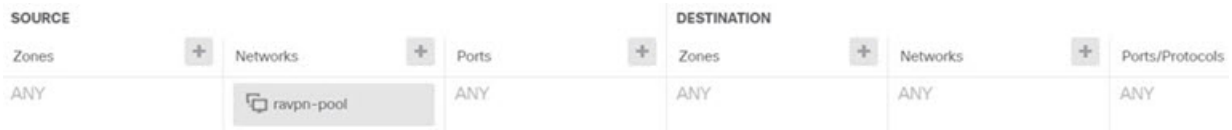
ステップ 3 （接続プロファイルで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] を設定していない場合。）リモート アクセス VPN アドレス プールからのアクセスを許可するアクセス制御ルールを設定します。

接続プロファイルで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] を選択した場合、RA VPN プールアドレスからのトラフィックは、アクセス制御ポリシーをバイパスします。このトラフィックに適用されるアクセス制御ルールを作成することはできません。オプションを無効にした場合にのみ、ルールを作成する必要があります。

次の例では、アドレス プールから任意の宛先へのトラフィックが許可されます。これは、ユーザ固有の要件を満たすように調整できます。不要なトラフィックを除外するブロック ルールをルールの前に置くことができます。

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

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



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

d) **[OK]** をクリックします。

ステップ 4 変更を保存します。

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

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

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

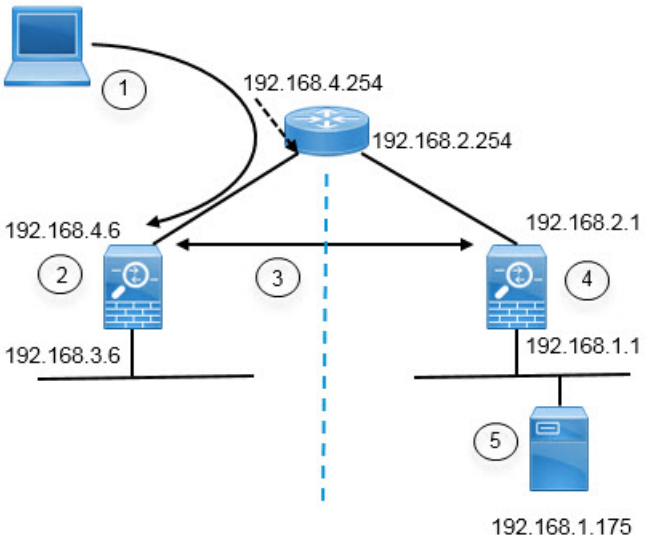
リモート アクセス VPN を使用した外部ネットワークでのディレクトリ サーバの使用法

リモート アクセス VPN を設定し、モバイル ワーカーや在宅勤務者に対して内部ネットワークへのセキュア接続を許可できます。接続のセキュリティはディレクトリ サーバに応じて異なります。セキュリティ サーバは、許可されたユーザだけがアクセスできるようにユーザ接続を認証します。

ディレクトリ サーバが内部ネットワークではなく外部ネットワークにある場合は、外部インターフェイスからディレクトリ サーバがあるネットワークへのサイト間 VPN 接続を設定する必要があります。**サイト間 VPN 設定におけるヒント**：リモート アクセス VPN デバイスの外部インターフェイス アドレスを、サイト間 VPN 接続の「内部」ネットワークと、ディレクトリ サーバの前に位置するデバイスのリモート ネットワークに含める必要があります。これについては、次の手順で詳しく説明します。

（注） 仮想管理インターフェイスのゲートウェイとしてデータ インターフェイスを使用する場合には、この設定によりアイデンティティ ポリシーにディレクトリを使用できるようになります。管理ゲートウェイとしてデータ インターフェイスを使用しない場合は、管理ネットワークから、サイト間 VPN 接続に参加する内部ネットワークへのルートがあることを確認してください。

この使用例では次のネットワーク シナリオが実現します。



図のコールアウト	説明
1	192.168.4.6 へ VPN 接続するリモート アクセス ホスト。クライアントは 172.18.1.0/24 アドレス プールのアドレスを取得します。
2	サイト A：リモート アクセス VPN をホストします。
3	サイト A とサイト B の 脅威に対する防御 デバイスの外部インターフェイス間のサイト間 VPN トンネル。
4	サイト B：ディレクトリ サーバをホストします。
5	サイト B の内部ネットワーク上のディレクトリ サーバ。

始める前に

この使用例では、デバイス設定ウィザードで標準のベースライン構成が完了していることを前提としています。詳細：

- inside_zone から outside_zone へのトラフィックを許可（または信頼）する Inside_Outside_Rule アクセス制御ルールが設定されている。
- inside_zone セキュリティ ゾーンに内部インターフェイス、outside_zone セキュリティ ゾーンに外部インターフェイスが含まれている。
- 内部インターフェイスから外部インターフェイスへ流れるすべてのトラフィックに対してインターフェイス PAT を実行する InsideOutsideNATRule がある。デフォルトで内部ブリッジ グループを使用するデバイスには、インターフェイス PAT に関する複数のルールが設定されていることがあります。
- 外部インターフェイスを指す 0.0.0.0/0 のスタティック IPv4 ルートがある。この例では、外部インターフェイスにスタティック IP アドレスを使用することを前提としていますが、

DHCP を使用してスタティック ルートを動的に取得することもできます。この例では、次のスタティック ルートが想定されます。

- サイト A：外部インターフェイス、ゲートウェイは 192.168.4.254 です。
- サイト B：外部インターフェイス、ゲートウェイは 192.168.2.254 です。

手順

ステップ 1 ディレクトリ サーバをホストする**サイト B** でサイト間 VPN 接続を設定します。

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

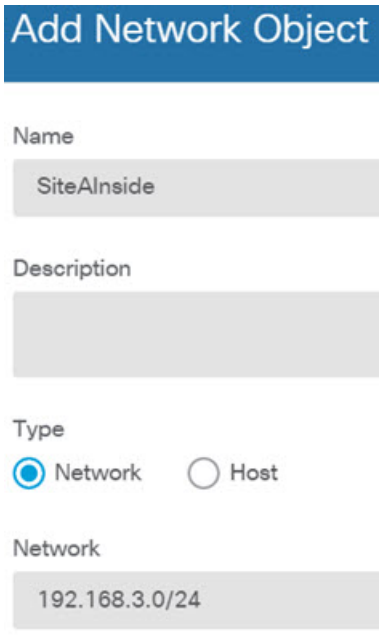
b) **[+]**ボタンをクリックします。

c) [エンドポイント設定（Endpoint Settings）] の次のオプションを設定します。

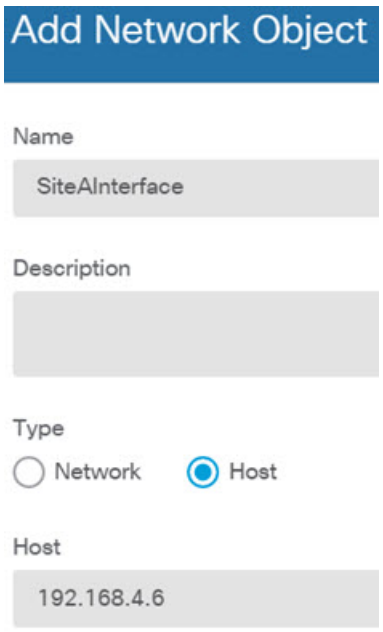
- [接続プロファイル名（Connection Profile Name）]：名前を入力します。例えば、（サイト A への接続を示す）SiteA と入力します。
- [ローカル サイト（Local Site）]：以下のオプションによってローカル エンドポイントを定義します。
  - [ローカル VPN アクセス インターフェイス（Local VPN Access Interface）]：**outside** インターフェイス（図でアドレスが 192.168.2.1 のインターフェイス）を選択します。
  - [ローカル ネットワーク（Local Network）]：[+] をクリックし、VPN 接続に参加させるローカル ネットワークを特定するネットワーク オブジェクトを選択します。ディレクトリ サーバは、このネットワーク上にあるのでサイト間 VPN に参加できます。オブジェクトがまだ存在していない場合には、[新しいネットワークの作成（Create New Network）] をクリックし、192.168.1.0/24 ネットワークのオブジェクトを設定します。オブジェクトを保存した後で、ドロップダウンリストからそのオブジェクトを選択し、[OK] をクリックします。

- [リモート サイト（Remote Site）]：以下のオプションによってリモート エンドポイントを定義します。
  - [リモート IP アドレス（Remote IP Address）]：192.168.4.6（VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレス）を入力します。
  - [リモート ネットワーク（Remote Network）]：[+] をクリックし、VPN 接続に参加させるリモート ネットワークを特定するネットワーク オブジェクトを選択します。[新しいネットワークの作成（Create New Network）] をクリックし、以下のオブジェクトを設定し、リストからこれらのオブジェクトを選択します。

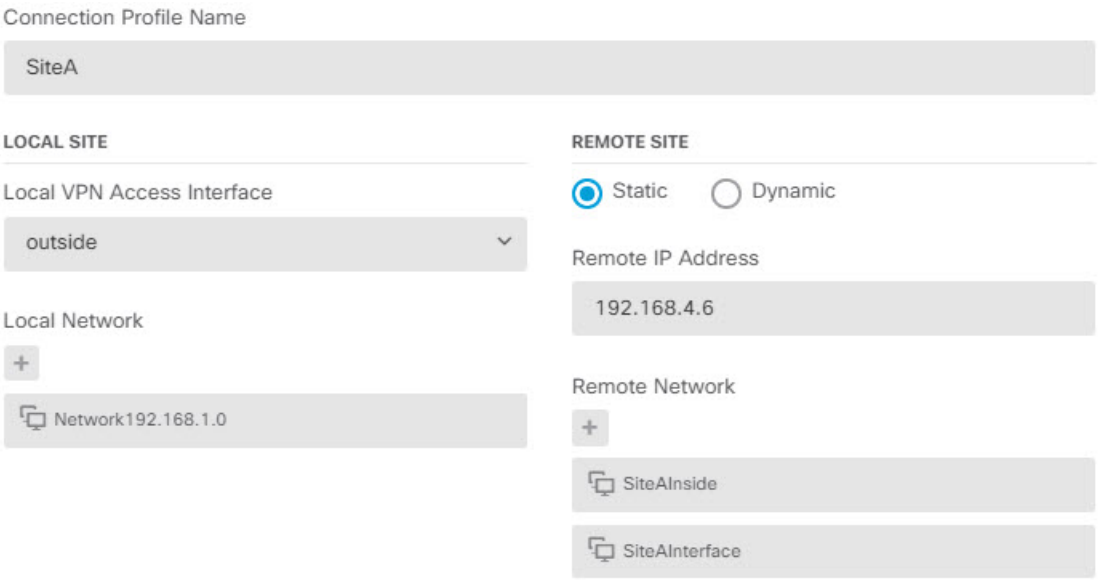
    1. SiteAInside、Network、192.168.3.0/24.



2. SiteAInterface、Host、192.168.4.6.ヒント：リモート アクセス VPN 接続ポイントのアドレスを、サイト間 VPN 接続のリモート ネットワークの一部として含める必要があります。これにより、そのインターフェイスでホストされている RA VPN がディレクトリ サーバを使用できるようになります。



終了すると、エンドポイント設定は次のようになります。



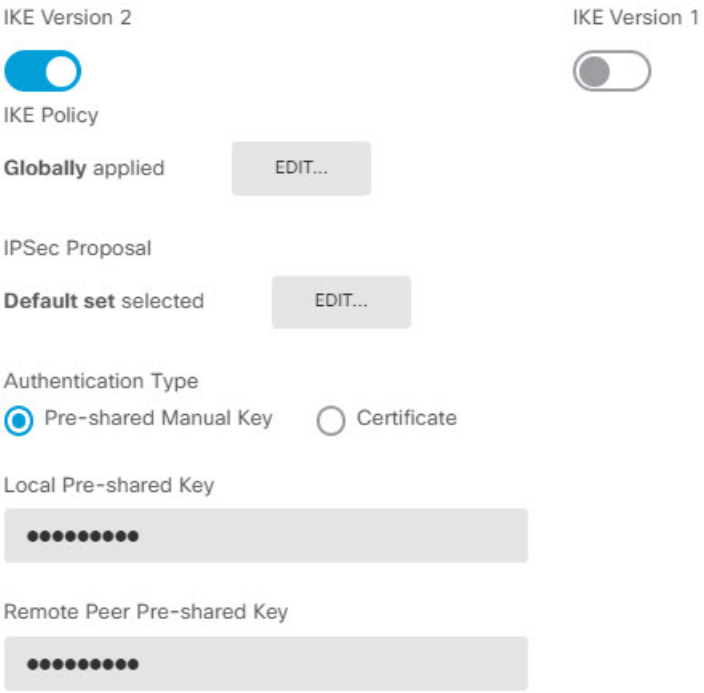
d) [次へ（Next）] をクリックします。

e) VPN のプライバシー設定を定義します。

この使用例では、エクスポート制御機能を使用できる資格があり、これにより強力な暗号化が使用可能であることを前提としています。各自のニーズとライセンス コンプライアンスに合わせて次に示す設定例を調整してください。

- [IKE バージョン 2（IKE Version 2）]、[IKE バージョン 1（IKE Version 1）] : デフォルトのままにします（[IKE バージョン 2（IKE Version 2）] は有効、[IKE バージョン 1（IKE Version 1）] は無効）。
- [IKE ポリシー（IKE Policy）] : [編集（Edit）] をクリックし、[AES-GCM-NULL-SHA] と [AES-SHA-SHA] を有効にし、[DES-SHA-SHA] を無効にします。
- [IPsec プロポーザル（IPsec Proposal）] : [編集（Edit）] をクリックします。[IPsec プロポーザル（IPsec Proposal）] ダイアログボックスで [+] をクリックし、次に [デフォルトを設定（Set Default）] を選択してデフォルトの AES-GCM プロポーザルを選択します。
- [ローカル事前共有キー（Local Preshared Key）]、[リモート ピア事前共有キー（Remote Peer Preshared Key）] : このデバイスとリモート デバイスで VPN 接続に対して定義されているキーを入力します。IKEv2 では異なるキーを使用できます。キーは 1 ～ 127 文字の英数字で指定できます。**サイト A のデバイスでサイト間 VPN 接続を作成するときに同じ文字列を設定する必要があるため、これらのキーは覚えておいてください。**

IKE ポリシーは次のようになります。



f) [追加オプション（Additional Options）] を設定します。

- [NAT 免除（NAT Exempt）]：内部ネットワークをホストするインターフェイス（この例では **inside** インターフェイス）を選択します。通常、サイト間 VPN トンネル内のトラフィックで IP アドレスを変換することは推奨されません。このオプションは、ローカル ネットワークが（ブリッジ グループ メンバーではなく）単一のルーテッドインターフェイスの背後にある場合にのみ機能します。ローカル ネットワークが複数のルーテッド インターフェイスの背後にある場合、または 1 つ以上のブリッジ グループ メンバーになっている場合は、手動で NAT 免除ルールを作成する必要があります。必要なルールを手動で作成する方法については、NAT からのサイト間 VPN トラフィックの免除を参照してください。
- [Perfect Forward Secrecy 用 Diffie-Hellman グループ（Diffie-Helman Group for Perfect Forward Secrecy）]：[グループ 19（Group 19）] を選択します。このオプションは、暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用するかどうかを指定します。一意のセッション キーを使用することによって、以降の復号から交換が保護されます。このことは、交換全体が記録され、攻撃者がエンドポイント デバイスで使用される事前共有キーまたは秘密キーを入手している場合であっても該当します。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。

オプションは次のようになります。

g) [次へ（Next）] をクリックします。

h) 概要を確認してから [完了（Finish）] をクリックします。

概要情報はクリップボードにコピーされます。この情報をドキュメントに貼り付けて、リモート ピアを設計する際の参考にしたり、ピアの設定担当者に送信したりできます。

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

j) [今すぐ展開（Deploy Now）] ボタンをクリックして、導入が正常に完了するまで待ちます。

これでサイト B デバイスがサイト間 VPN 接続の片側をホストできるようになりました。

ステップ 2 **サイト B** デバイスからログアウトし、**サイト A** デバイスにログインします。

ステップ 3 リモート アクセス VPN をホストする**サイト A** でサイト間 VPN 接続を設定します。

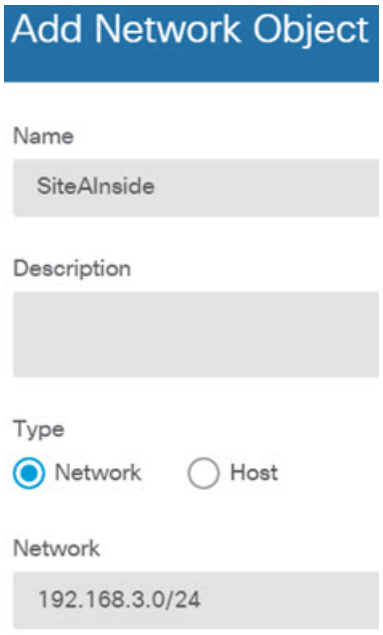
a) **[デバイス（Device）]**をクリックし、次に [サイト間 VPN（Site-to-Site VPN）] グループの [設定の表示（View Configuration）] をクリックします。

b) **[+]**ボタンをクリックします。

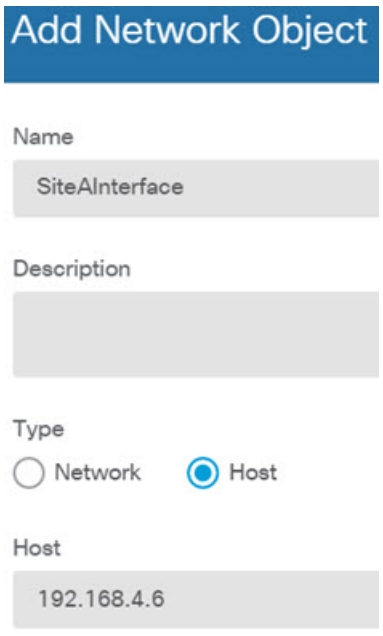
c) [エンドポイント設定（Endpoint Settings）] の次のオプションを設定します。

- [接続プロファイル名（Connection Profile Name）]：名前を入力します。たとえば、サイト B への接続を示す SiteB と入力します。
- [ローカル サイト（Local Site）]：以下のオプションによってローカル エンドポイントを定義します。
  - [ローカル VPN アクセス インターフェイス（Local VPN Access Interface）]：**outside** インターフェイス（図でアドレスが 192.168.4.6 のインターフェイス）を選択します。
  - [ローカル ネットワーク（Local Network）]：[+] をクリックし、VPN 接続に参加させるローカル ネットワークを特定するネットワーク オブジェクトを選択します。[新しいネットワークの作成（Create New Network）] をクリックし、以下のオブジェクトを設定し、リストからこれらのオブジェクトを選択します。**サイト B のデバイスに同じオブジェクトを作成しましたが、サイト A のデバイスでも再度同じオブジェクトを作成する必要があります。**

    1. SiteAInside、Network、192.168.3.0/24.



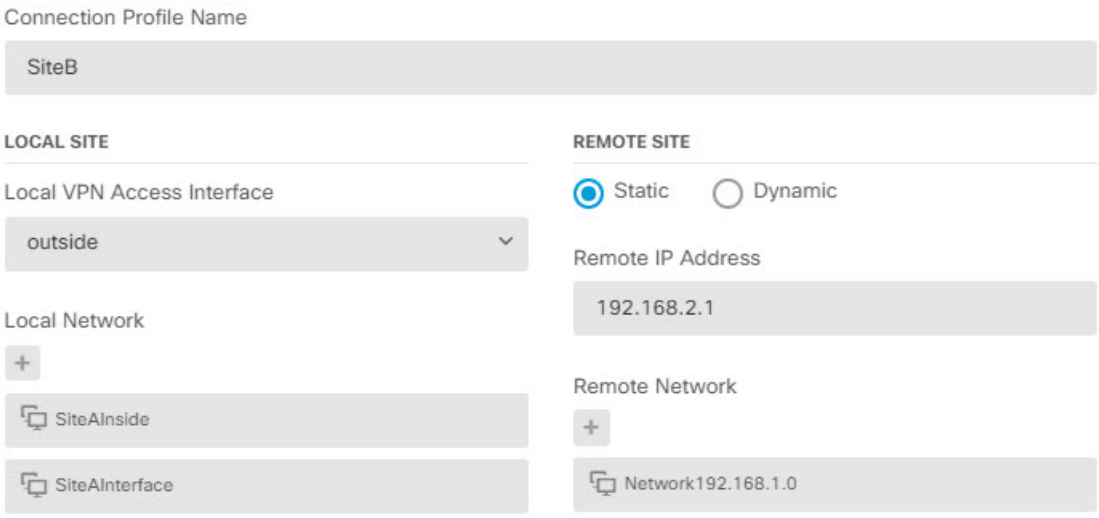
2. SiteAInterface、Host、192.168.4.6.ヒント：リモート アクセス VPN 接続ポイントのアドレスを、サイト間 VPN 接続の内部ネットワークの一部として含める必要があります。これにより、そのインターフェイスでホストされている RA VPN がリモート ネットワークのディレクトリ サーバを使用できるようになります。



- [リモート サイト（Remote Site）]：以下のオプションによってリモート エンドポイントを定義します。

- [リモート IP アドレス（Remote IP Address）]：192.168.2.1（VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレス）を入力します。
- [リモート ネットワーク（Remote Network）]：[+] をクリックし、VPN 接続に参加させるリモート ネットワーク（ディレクトリ サーバを含むネットワーク）を特定するネットワーク オブジェクトを選択します。[新しいネットワークの作成（Create New Network）] をクリックし、192.168.1.0/24 ネットワークのオブジェクトを設定します。オブジェクトを保存した後で、ドロップダウンリストからそのオブジェクトを選択し、[OK] をクリックします。**サイト B のデバイスに同じオブジェクトを作成しましたが、サイト A のデバイスでも再度同じオブジェクトを作成する必要があります。**

終了すると、エンドポイント設定は次のようになります。サイト B の設定と比較すると、ローカル/リモート ネットワークで逆の設定が使用されていることに注意してください。ポイントツーポイント接続の両端がこのようになります。

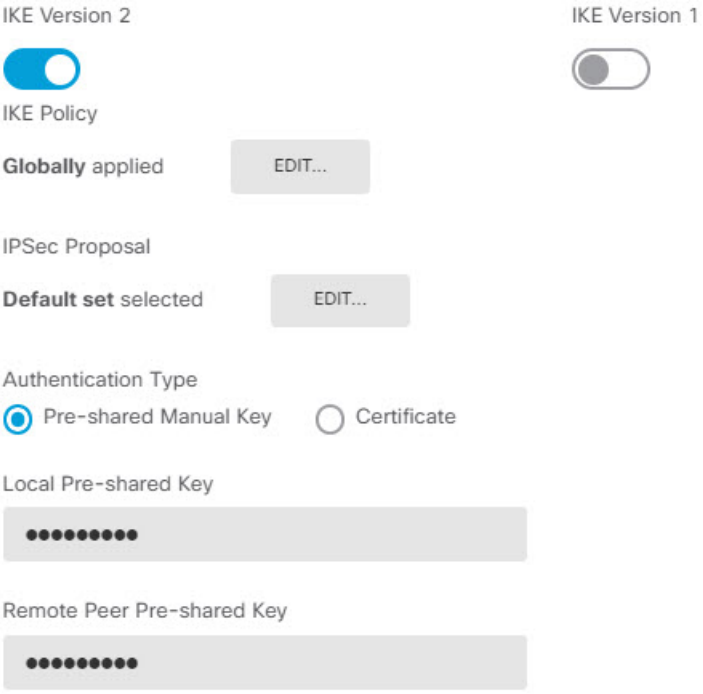


d) [次へ（Next）] をクリックします。

e) VPN のプライバシー設定を定義します。

サイト B 接続と同じ IKE バージョン、ポリシー、および IPsec プロポーザル、同じ事前共有キーを設定しますが、**ローカルとリモートの事前共有キーが逆になっていることを確認してください。**

IKE ポリシーは次のようになります。



f) [追加オプション（Additional Options）] を設定します。

- [NAT 免除（NAT Exempt）]：内部ネットワークをホストするインターフェイス（この例では**inside**インターフェイス）を選択します。通常、サイト間 VPN トンネル内のトラフィックで IP アドレスを変換することは推奨されません。このオプションは、ローカル ネットワークが（ブリッジ グループ メンバーではなく）単一のルーテッドインターフェイスの背後にある場合にのみ機能します。ローカル ネットワークが複数のルーテッド インターフェイスの背後にある場合、または 1 つ以上のブリッジ グループ メンバーになっている場合は、手動で NAT 免除ルールを作成する必要があります。必要なルールを手動で作成する方法については、NAT からのサイト間 VPN トラフィックの免除を参照してください。
- [Perfect Forward Secrecy 用 Diffie-Hellman グループ（Diffie-Helman Group for Perfect Forward Secrecy）]：[グループ 19（Group 19）] を選択します。

オプションは次のようになります。

g) [次へ（Next）] をクリックします。
h) 概要を確認してから [完了（Finish）] をクリックします。
i) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

j) [今すぐ展開（Deploy Now）] ボタンをクリックして、導入が正常に完了するまで待ちます。

これでサイト A デバイスがサイト間 VPN 接続のもう一方の側をホストできるようになりました。サイト B は互換性のある設定を使用してすでに設定されているため、2 つのデバイスが VPN 接続をネゴシエートします。

接続を確認するには、デバイス CLI にログインし、ディレクトリ サーバに対して ping を実行します。**show ipsec sa**コマンドを使用して、セッション情報を表示することもできます。

ステップ 4 **サイト A** のディレクトリ サーバを設定します。[テスト（Test）] をクリックして、接続があることを確認します。

a) [オブジェクト（Objects）] を選択し、目次から [アイデンティティレルム（Identity Realm）][アイデンティティソース（Identity Sources）] を選択します。
b) **[+]** > **[AD]** をクリックします。
c) 基本レルムのプロパティを設定します。

- [名前（Name）]：ディレクトリ レルムの名前。たとえば、AD などです。

- [タイプ（Type）]：ディレクトリ サーバのタイプ。サポートされているタイプはActive Directory のみのため、このフィールドは変更できません。
- [ディレクトリユーザ名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。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）。

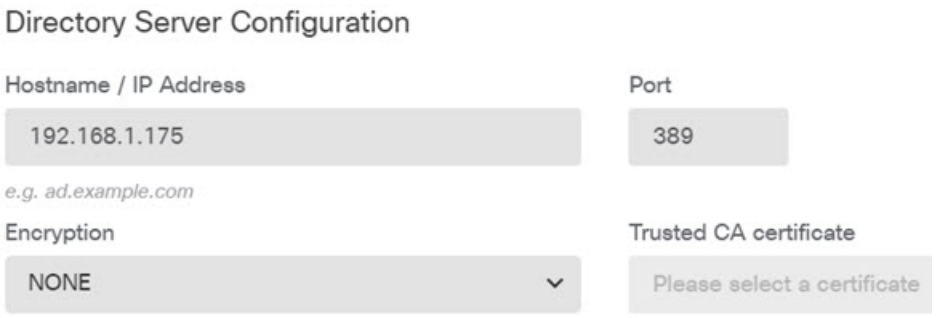
  （注）
  この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=adminisntrator,cn=users,dc=example,dc=com と変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [ベースDN（Base DN）]：ユーザおよびグループ情報、つまり、ユーザ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。たとえば、cn=users,dc=example,dc=com となります。ベース DN の検索方法については、ディレクトリ ベース DN の決定を参照してください。
- [AD プライマリ ドメイン（AD Primary Domain）]：デバイスが参加する必要のある、完全修飾 Active Directory ドメイン名。たとえば、example.com のように指定します。

d) 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/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。この例では、192.168.1.175 と入力します。
- [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。LDAPS を暗号化方式に選択している場合は、ポート 636 を使用します。この例では 389 のままにします。

- [暗号化（Encryption）]：ユーザとグループ情報をダウンロードするときに暗号化接続を使用します。デフォルトは[なし（None）]です。したがって、ユーザとグループ情報はクリアテキストでダウンロードされます。RA VPN の場合は[LDAPS]（LDAP over SSL）を使用できます。このオプションを選択する場合はポート 636 を使用します。RA VPN は STARTTLS をサポートしていません。この例では[なし（None）]を選択します。
- [信頼できる CA 証明書（Trusted CA Certificate）]：暗号化方式を選択した場合は、認証局（CA）証明書をアップロードして、システムとディレクトリ サーバの間で信頼できる接続を有効化します。認証に証明書を使用している場合、証明書のサーバ名とサーバのホスト名/IP アドレスが一致する必要があります。たとえば、IP アドレスとして 192.168.1.175 を使用し、証明書内で ad.example.com を使用した場合は、接続が失敗します。



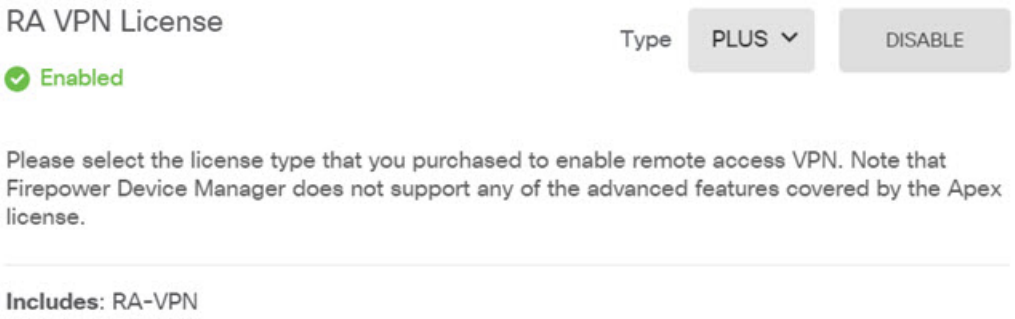
e) システムがサーバと通信できるか確認するには、[テスト（Test）]ボタンをクリックします。

システムは別個のプロセスを使用してサーバにアクセスします。このため、アイデンティティ ポリシーでは接続に成功してリモート アクセス VPN では失敗するなど、ある使用方法では接続が成功しても、別の方法では失敗したことを示すエラーが表示される場合があります。サーバにアクセスできない場合は、指定した IP アドレスとホスト名が正しく、DNS サーバにそのホスト名が入力されているかなどを確認します。また、サイト間 VPN 接続が機能しており、VPN にサイト A の外部インターフェイス アドレスを含めており、NAT がディレクトリ サーバのトラフィックを変換していないことを確認します。サーバのスタティック ルートを設定することが必要な場合もあります。

f) [OK]をクリックします。

ステップ 5 **[デバイス（Devices）] > [スマート ライセンス（Smart License）] > [設定の表示（View Configuration）]** をクリックし、RA VPN ライセンスを有効にします。

RA VPN ライセンスを有効にする場合は、購入したライセンスのタイプ（Plus、Apex（または両方）、VPN Only）を選択します。詳細については、リモート アクセス VPN のライセンス要件 （9 ページ）を参照してください。

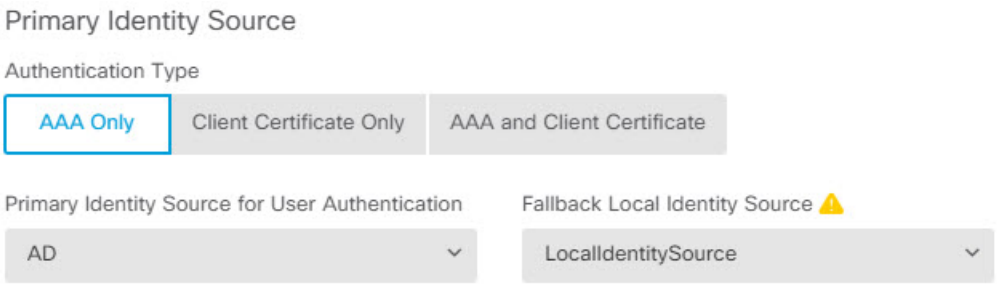


ステップ 6 サイト A のリモート アクセス VPN を設定します。

a) **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。[接続プロファイル（Connection Profiles）] ページを表示していることを確認します。

b) 接続プロファイルを作成または編集します。

c) ウィザードの最初のステップでプロファイル名を設定し、その後にプライマリ認証ソースとして AD レルムを選択します。必要に応じて、フォールバック アイデンティティ ソースとしてローカルデータベースを選択できます。



d) アドレスプールを設定します。

この例では、[+] をクリックしてから IPv4 アドレスプールで [新しいネットワークの作成（Create New Network）] を選択し、172.18.1.0/24 ネットワークのオブジェクトを作成し、そのオブジェクトを選択します。クライアントには、このプールからアドレスが割り当てられます。IPv6 プールは空白のままにします。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アドレス プールを指定することはできません。

オブジェクトは次のようになります。

プールの仕様は次のようになります。

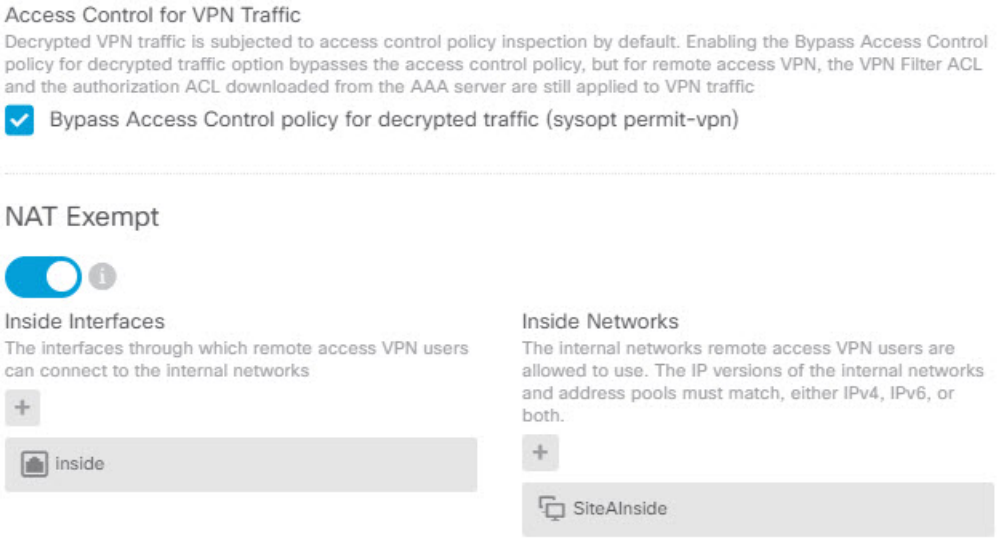
e) [次へ（Next）] をクリックし、適切なグループポリシーを選択します。

選択したポリシーに関する要約情報を確認します。DNSサーバが設定されていることを確認します。設定されていない場合は、ここでポリシーを編集して、DNSを設定します。

f) [次へ（Next）] をクリックし、[グローバル設定（Global Settings）] で [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択し、[NAT免除（NAT Exempt）] オプションを設定します。

[NAT免除（NAT Exempt）] では、次のオプションを設定する必要があります。他に定義済みの接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。

- [内部インターフェイス（Inside Interfaces）]：[内部（inside）] インターフェイスを選択します。これらは、リモート ユーザがアクセスする内部ネットワークのインターフェイスです。これらのインターフェイスに関する NAT ルールが作成されます。
- [内部ネットワーク（Inside Networks）]：SiteAInside ネットワーク オブジェクトを選択します。これらは、リモート ユーザがアクセスする内部ネットワークを表すネットワーク オブジェクトです。



g) サポートするプラットフォームの セキュアクライアント パッケージをアップロードします。

h) [次へ（Next）] をクリックして、設定を確認します。

最初に、サマリーが正しいことを確認します。

次に、[手順（Instructions）] をクリックして、セキュアクライアント 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します。[コピー（Copy）] をクリックして、それらの手順をクリップボードにコピーし、テキスト ファイルまたは電子メールに貼り付けます。

i) **[終了]** をクリックします。

ステップ 7 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

ステップ 8 [今すぐ展開（Deploy Now）] ボタンをクリックして、導入が正常に完了するまで待ちます。

これで、サイト A のデバイスが RA VPN の接続を承認できるようになりました。外部ユーザーに セキュアクライアント クライアントをインストールさせて、VPN 接続を完了させます。

接続を確認するには、デバイス CLI にログインし、**show vpn-sessiondb anyconnect** コマンドを使用してセッション情報を表示します。

グループによって RA VPN アクセスを制御する方法

リモートアクセス VPN 接続プロファイルを、グループポリシーに基づいて内部リソースへの差分アクセスを提供するように設定することができます。たとえば、従業員に無制限のアクセスを提供し、請負業者には単一の内部ネットワーク以外へのアクセスを提供したくない場合

は、グループポリシーを使用して、適切にアクセスを制限するための異なる ACL を定義できます。

次の例は、192.168.2.0/24 内部サブネットにのみアクセスする必要がある請負業者の RA VPN 接続の設定方法を示しています。通常の従業員の場合、VPN に対してトラフィックフィルタが定義されていないデフォルトグループポリシーを使用できます。デフォルトグループポリシーを編集してこれらのユーザに制限を適用し、次のように構築された ACL を適用することができます。

始める前に

次の手順では、請負業者に使用するアイデンティティソースがすでに作成されていると仮定します。これは、通常の従業員に使用するものとは異なるソースである可能性があります。アイデンティティソースはアクセスの制限に厳密に関連するものではないため、この例からは省略します。

また、この例では、「inside2」インターフェイスが 192.168.2.0/24 サブネットを IP アドレス 192.168.2.1 でホストするように設定されていると想定します（サブネット上のその他のアドレスも許容されます）。

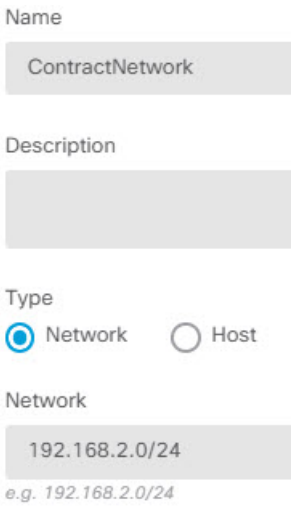
手順

ステップ 1 RA VPN トラフィックを制限するため、拡張アクセスコントロールリスト（ACL）を設定します。

まず、ターゲット 192.168.2.0/24 を定義するネットワークオブジェクトを設定し、次にアクセスリストを定義するスマート CLI オブジェクトを作成する必要があります。ACL の最後には暗黙の「deny」があるため、サブネットへのアクセスを許可することだけが必要となります。サブネット外の IP アドレスへのトラフィックは拒否されます。この例は、IPv4 のみに適用されます。また、特定のサブネットへの IPv6 アクセスを制限するためのオブジェクトも設定できます。ネットワークオブジェクトを作成し、同じ ACL に IPv6 ベースの ACE を追加するだけです。

a) **[オブジェクト]** > **[ネットワーク]**を選択し、必要なオブジェクトを作成します。

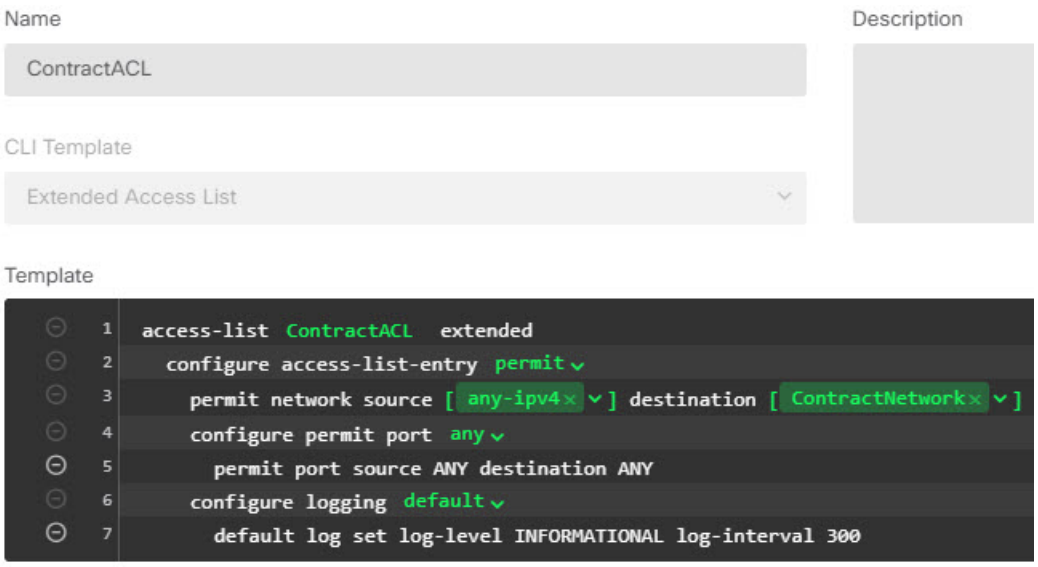
たとえば、オブジェクトに ContractNetwork という名前を付けます。このオブジェクトは次のようになります。



b) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[Smart CLI]** > **[オブジェクト（Objects）]** を選択します。
c) [+] をクリックして新しいオブジェクトを作成します。
d) ACL の名前を入力します。**ContractACL** などを入力します。
e) [CLI テンプレート（CLI Template）] の場合は、[拡張アクセスリスト（Extended Access List）] を選択します。
f) [テンプレート（Template）] 本文で次のように設定します。

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = ContractNetwork object
- configure permit port = any
- configure logging = default

ACE は次のようになります。



g) [OK]をクリックします。

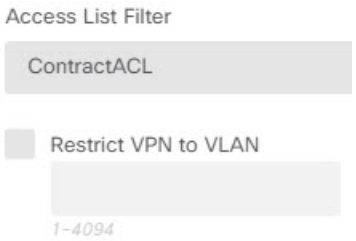
この ACL は、次に変更を展開するときに設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

ステップ 2 ACL を使用するグループポリシーを作成します。

最低限として、グループ ポリシーの DNS サーバを設定する必要もあります。必要に応じて他のオプションを設定できます。次の手順は、この使用例に関連する 1 つの設定に重点を置いています。

a) **[デバイス（Device）]** > **[RA VPN]** > **[グループポリシー（Group Policies）]** を選択します。
b) [+] をクリックして新しいグループポリシーを作成します。
c) [全般（General）] ページで、ポリシーの名前（**ContractGroup** など）を入力します。
d) 目次で[トラフィックフィルタ]をクリックします。
e) [アクセスリストフィルタ（Access List Filter）] の場合は、ContractACL オブジェクトを選択します。

この例では、VLAN オプションは空のままにします。別の方法として、フィルタリング用の VLAN を設定し、その VLAN にサブインターフェイスを設定することも可能です。



f) [OK] をクリックして、グループポリシーを保存します。

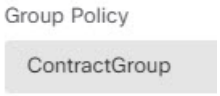
ステップ 3 コントラクタの接続プロファイルを設定します。

a) [RA VPN] ページで、目次の [接続プロファイル（Connection Profiles）] をクリックします。
b) 新しい接続プロファイルを作成するには、[+]をクリックします。
c) ウィザードのステップ 1 を完了し、[次へ（Next）] をクリックします。

プロファイルの名前（Contractors など）を入力します。

残りのオプションを通常どおりに設定します。これには、請負業者の適切な認証ソースの選択、アドレスプールの定義が含まれます。

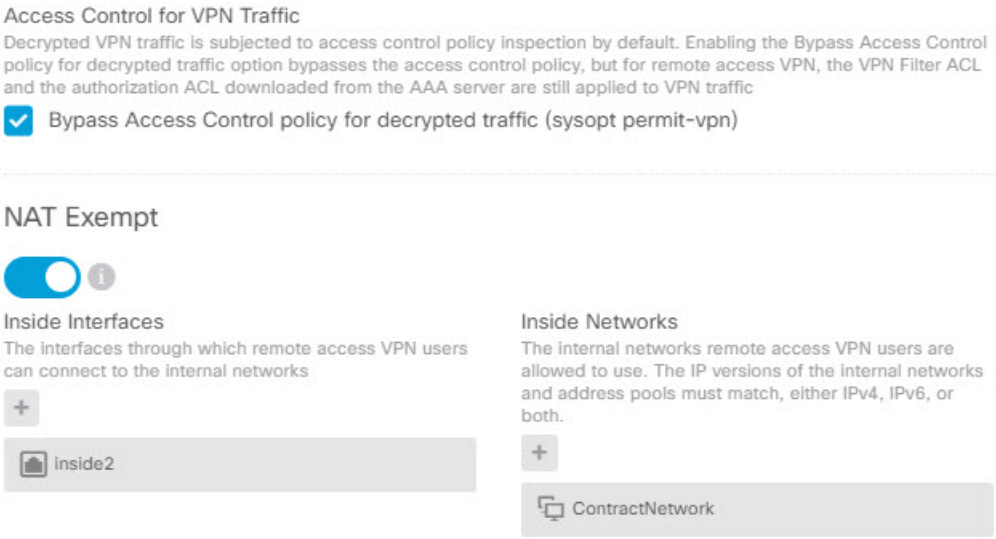
d) 請負業者用に設定されているグループポリシーを選択し、[次へ（Next）] をクリックします。



e) グローバル設定で、[復号されたトラフィックでアクセスコントロール ポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn）] オプションを選択し、[NAT免除（NAT Exempt）] オプションを設定します。

[NAT免除（NAT Exempt）] では、次のオプションを設定する必要があります。他に定義済みの接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。

- [内部インターフェイス（Inside Interfaces）]：**inside2** インターフェイスを選択します。これらは、リモート ユーザがアクセスする内部ネットワークのインターフェイスです。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）]：ContractNetwork ネットワーク オブジェクトを選択します。これらは、リモート ユーザがアクセスする内部ネットワークを表すネットワーク オブジェクトです。



f) サポートするプラットフォームの セキュアクライアント パッケージをアップロードします。

g) [次へ（Next）] をクリックして、設定を確認します。

最初に、サマリーが正しいことを確認します。

次に、[手順（Instructions）] をクリックして、セキュアクライアント 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します。[コピー（Copy）] をクリックして、それらの手順をクリップボードにコピーし、テキスト ファイルまたは電子メールに貼り付けます。

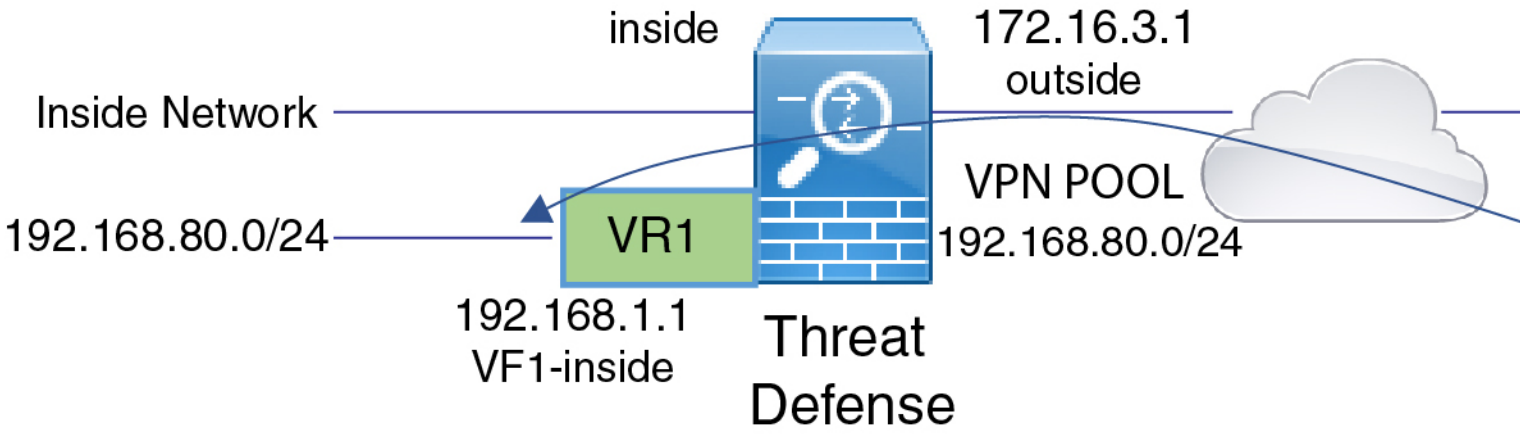
h) **[完了（Finish）]** をクリックします。

異なる仮想ルータの内部ネットワークへの RA VPN アクセスを可能にする方法

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

仮想ルータのルーティングテーブルはそれぞれ異なるため、RA VPN ユーザが別の仮想ルータの一部であるネットワークにアクセスする必要がある場合には、スタティックルートを作成する必要があります。

次の例について考えます。RA VPN ユーザが 172.16.3.1 の外部インターフェイスに接続するとします。このユーザには192.168.80.0/24 のプールに含まれる IP アドレスが割り当てられます。その結果、このユーザは、グローバル仮想ルータに接続されている内部ネットワークにアクセスできるようになります。ただし、仮想ルータ VR1 の一部である 192.168.1.0/24 ネットワークに到達することはできません。VR1 ネットワークと RA VPN ユーザ間のトラフィックフローを許可するには、双方向のスタティックルートを設定する必要があります。



始める前に

この例では、すでにRA VPNを設定し、仮想ルータを定義し、インターフェイスを設定して適切な仮想ルータに割り当てていることを前提としています。

手順

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

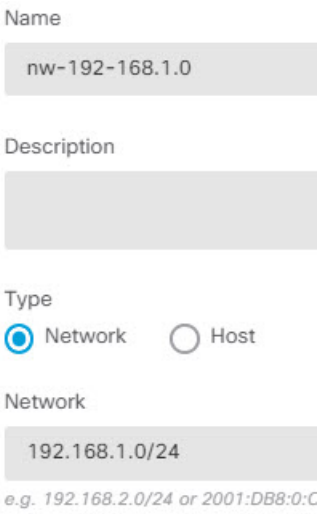
このルートにより、VPN プール内の IP アドレスが割り当てられた セキュアクライアントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできるようになります。

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

b) グローバル仮想ルータの表示アイコン（  ）をクリックします。

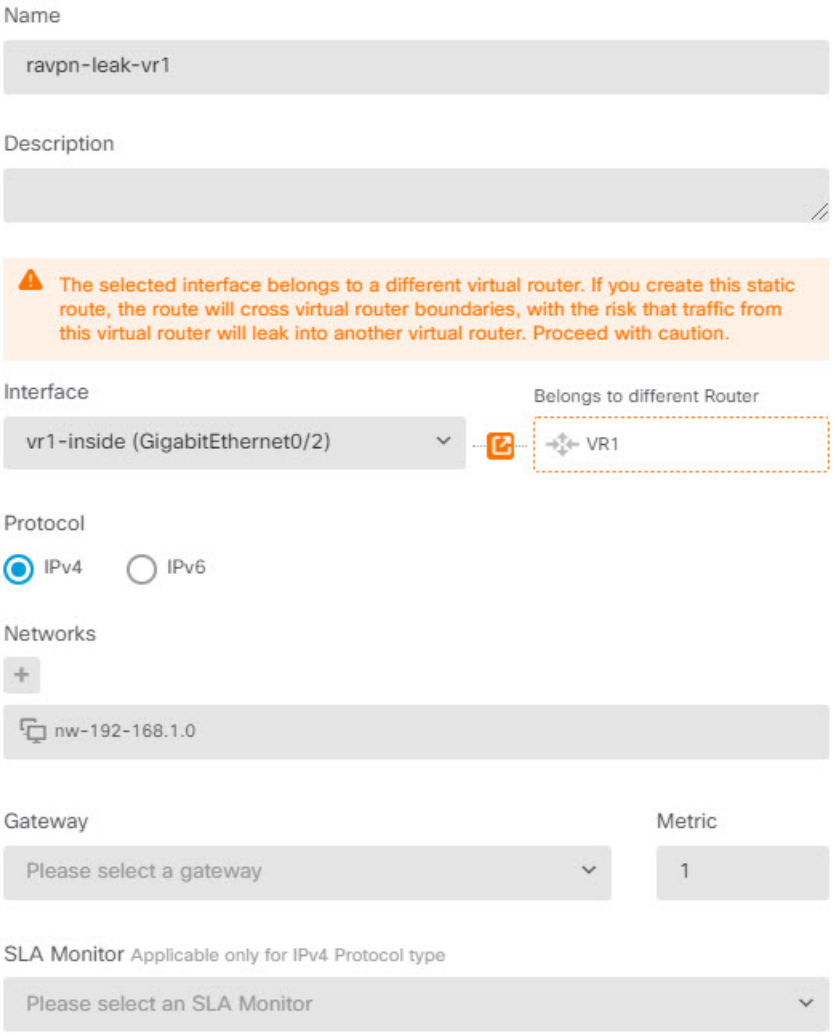
c) グローバルルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：任意の名前（**ravpn-leak-vr1** など）を付けることができます。
- [インターフェイス（Interface）]：**vr1-inside** を選択します。
- [プロトコル（Protocol）]：**IPv4** を選択します。
- [ネットワーク（Networks）]：192.168.1.0/24 ネットワークを定義するオブジェクトを選択します。必要な場合には、[新しいネットワークの作成（Create New Network）] をクリックしてオブジェクトを作成します。



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

次のようなダイアログが表示されるはずです。



d) [OK] をクリックします。

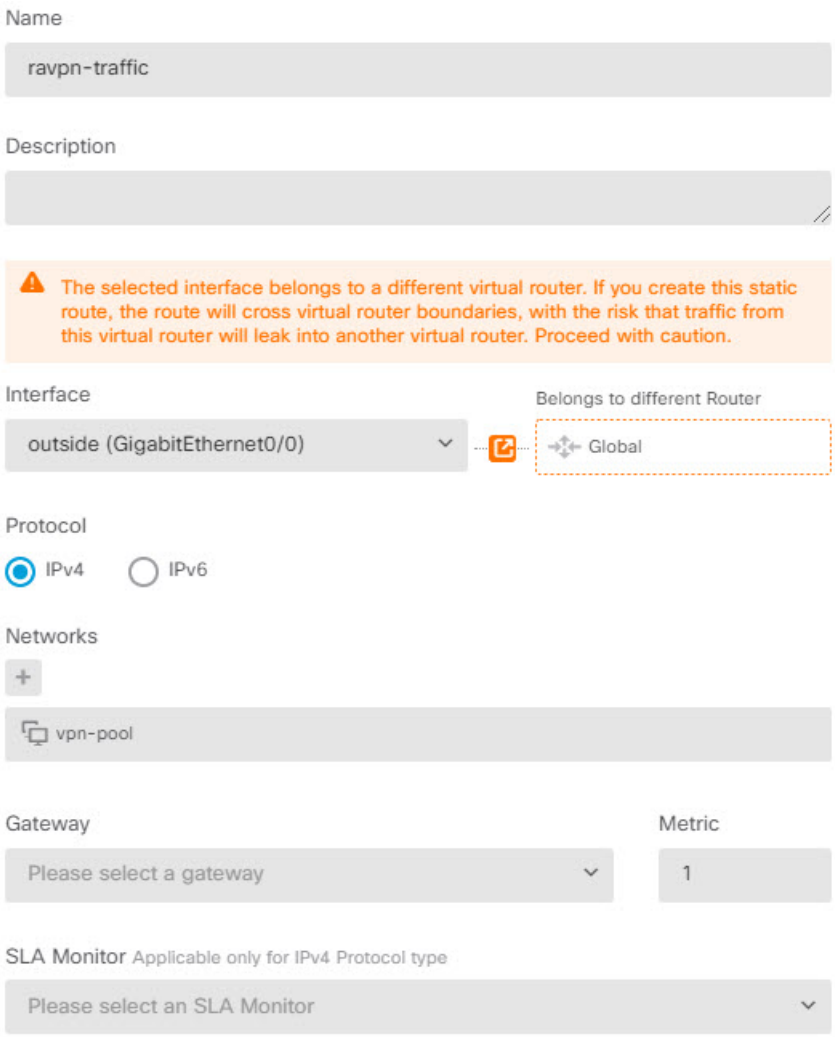
ステップ 2 VR1 からグローバル仮想ルータへのルートリークを設定します。

このルートにより、192.168.1.0/24 ネットワーク上のエンドポイントは、VPN プール内の IP アドレスが割り当てられた セキュアクライアントへの接続を開始できます。

a) 仮想ルータのドロップダウンリストから [VR1] を選択して、VR1 設定に切り替えます。
b) VR1 ルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。
   - [名前（Name）]：任意の名前（**ravpn-traffic** など）を付けることができます。
   - [インターフェイス（Interface）]：**outside** を選択します。
   - [プロトコル（Protocol）]：**IPv4** を選択します。
   - [ネットワーク（Networks）]：VPN プール用に作成したオブジェクト（**vpn-pool など**）を選択します。

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

次のようなダイアログが表示されるはずです。



c) [OK] をクリックします。

次のタスク

RA VPN アドレスプールとカスタム仮想ルータの IP アドレスの間に重複がある場合には、IP アドレスに対してスタティック NAT ルールを使用し、適切なルーティングを有効にする必要があります。とはいえ、単に重複しないようにRA VPNアドレスプールを変更する方がはるかに簡単です。

セキュアクライアント のアイコンとロゴをカスタマイズする方法

Windows および Linux クライアントマシン上の セキュアクライアント アプリケーションのアイコンとロゴをカスタマイズできます。アイコンの名前は事前定義されており、アップロードする画像のファイルタイプとサイズには特定の制限があります。

独自の実行可能ファイルを展開して GUI をカスタマイズする場合は、任意のファイル名を使用できますが、この例では、完全にカスタマイズされたフレームワークを展開せずに、アイコンとロゴを置き換えるだけであることを前提としています。

置き換えることができる画像はいくつかあり、それらのファイル名はプラットフォームによって異なります。カスタマイズオプション、ファイル名、タイプ、およびサイズの詳細については、『*Cisco Secure Client Administrator Guide*』の セキュアクライアントおよびインストーラのカスタマイズとローカライズに関する章を参照してください。たとえば、4.8 クライアントに関する章は次の場所にあります。

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

始める前に

この例では、Windows クライアントの次の画像を置き換えます。画像のサイズが最大サイズと異なる場合、自動的に最大サイズに変更され、必要に応じて画像が拡大されます。

- app_logo.png

  このアプリケーションロゴ画像はアプリケーションアイコンであり、最大サイズは 128 X 128 ピクセルです。

- company_logo.png

  この企業ロゴ画像は、トレイフライアウトと [詳細（Advanced）] ダイアログの左上隅に表示されます。最大サイズは 97 X 58 ピクセルです。

- company_logo_alt.png

  この代替企業ロゴ画像は、[バージョン情報（About）] ダイアログの右下隅に表示されます。最大サイズは 97 X 58 ピクセルです。

これらのファイルをアップロードするには、Threat Defense デバイスがアクセスできるサーバーにファイルを配置する必要があります。TFTP、FTP、HTTP、HTTPS、または SCP サーバを使用できます。これらのファイルから画像を取得するための URL には、サーバのセットアップで必要なパスとユーザ名/パスワードを含めることができます。この例では、TFTP を使用します。

手順

ステップ 1 カスタマイズされたアイコンとロゴを使用する必要がある、RA VPN ヘッドエンドとして機能している各 Threat Defense デバイスに画像ファイルをアップロードします。

a) SSH クライアントを使用してデバイス CLI にログインします。
b) CLI で、**system support diagnostic-cli** コマンドを入力して、診断 CLI モードを開始します。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv1>
```

（注）
メッセージに示されているように、診断 CLI を終了して通常の Threat Defense CLI モードに戻るには、**Ctrl + A キーを押してから D キーを押す**必要があります。

c) コマンドプロンプトに注意してください。通常の CLI では > だけが表示されますが、診断 CLI のユーザ EXEC モードではホスト名と > が表示されます。この例では、ftdv1> です。特権 EXEC モードを開始する必要があります。このモードでは、ftdv1# のように、# が終了文字として使用されます。プロンプトにすでに # が表示されている場合は、この手順をスキップしてください。それ以外の場合は、enable コマンドを入力し、パスワードプロンプトではパスワードを入力せずに単に Enter キーを押します。

```
ftdv1> enable
Password:
ftdv1#
```

d) **copy** コマンドを使用して、ホスティングサーバーから Threat Defense デバイスの disk0 に各ファイルをコピーします。それらのファイルは disk0:/anyconnect-images/ などのサブディレクトリに配置できます。**mkdir** コマンドを使用して新しいフォルダを作成できます。

たとえば、TFTP サーバの IP アドレスが 10.7.0.80 であり、新しいディレクトリを作成する場合、コマンドは次のようになります。最初の例の後は **copy** コマンドへの応答が省略されていることに注意してください。

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

ステップ 2 診断 CLI で **import webvpn** コマンドを使用して、セキュアクライアント に、それ自体のクライアントマシンへのインストール時にこれらの画像をダウンロードするように指示します。

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:**/*directoryname/filename*

このコマンドは Windows 用です。Linux の場合は、クライアントに応じて、**win** キーワードを **linux** または **linux-64** に置き換えます。

たとえば、前の手順でアップロードしたファイルをインポートする場合、まだ 診断 CLI だとすると、次のようになります。

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

ステップ 3 設定を確認します。

- インポートしたファイルを確認するには、診断 CLI の特権 EXEC モードで **show import webvpn AnyConnect-customization** コマンドを使用します。
- 画像がクライアントにダウンロードされたことは、ユーザがクライアントを実行したときに画像が表示されることで確認できます。Windows クライアントで次のフォルダを確認することもできます。ここで、%PROGRAMFILES% は、通常、c:\Program Files に置き換えられます。

  %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res

次のタスク

デフォルトの画像に戻す場合は、カスタマイズしたイメージごとに **revert webvpn** コマンドを（診断 CLI の特権 EXEC モードで）使用します。コマンドは次のとおりです。

revert webvpn AnyConnect-customization type resource platform win name *filename*

import webvpn の場合と同様に、当該のクライアント プラットフォームをカスタマイズしている場合は **win** を **linux** または **linux-64** に置き換え、インポートした画像ファイル名ごとに個別にコマンドを発行してください。例：

```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```

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。