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、各ユーザー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

Firewall Device Manager では、AnyConnect Client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。

AnyConnect Clientが Firewall 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Firewall 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VPNセッション数に上限が設けられます。この制限は、システム パフォーマンスが許容できないレベルに低下しないように設

計されています。この制限は、リモートアクセス VPN ユーザーとサイト間 VPN ピアを組み合わせたものです。これらの制限は、キャパシティ プランニングに使用します。

デバイス モデル	最大同時 VPN セッション数
ASA 5508-X	100
ASA 5516-X	300
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
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
FTDv：FTDv5	50
FTDv：FTDv10、FTDv20、FTDv30	250
FTDv：FTDv50	750
FTDv：FTDv100	10,000
ISA 3000	25

AnyConnect Client 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、AnyConnect Client 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 AnyConnect Client バージョンをダウンロードする必要があります。Firepower Threat Defense 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 AnyConnect Client 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。

AnyConnect Client 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。

AnyConnect Client 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 AnyConnect Client 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、Firewall Threat Defense デバイスから AnyConnect Client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。

AnyConnect Clientがすでにインストールされている場合、新しい AnyConnect Client 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 AnyConnect Client 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 Firewall Threat Defenseデバイスからユーザーに行ってもらう場合、以下の手順を実行するようにユーザーに指示します。

（注） Android および iOS のユーザーは、適切な App Store から AnyConnect Client 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、ユーザーは 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 AnyConnect Clientのバージョンがインストールされているかを確認します。AnyConnect Clientがユーザーのコンピュータにないか、下位のバージョンである場合、システムは自動的に AnyConnect Client ソフトウェアのインストールを開始します。

インストールが終了すると、AnyConnect Client 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ーの権限および属性の制御

外部 RADIUS サーバーまたは Firepower Threat Defense デバイスで定義されているグループポリシーから、RA VPN 接続にユーザーの認可属性（ユーザーの権利または権限とも呼ばれる）を適用できます。Firepower Threat Defense 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。

Firepower Threat Defense デバイスは次の順序で属性を適用します。

1. AAA サーバー上で定義されたユーザー属性：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。
2. Firepower Threat Defense デバイス上で設定されているグループポリシー：RADIUS サーバーからユーザーの RADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場合は、Firepower Threat Defense デバイスはそのユーザーを同じ名前のグループポリシーに入れて、そのグループポリシーの属性のうち、サーバーから返されないものを適用します。
3. 接続プロファイルによって割り当てられたグループポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザーに適用されるデフォルトのグループポリシーが含まれています。Firepower Threat Defense デバイスに接続するすべてのユーザーは、最初にこのグループに所属します。このグループでは、AAA サーバーから返されるユーザー属性、またはユーザーに割り当てられたグループポリシーにはない属性が定義されています。

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

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

RADIUS サーバーに送信された属性

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

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

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

RADIUS サーバーから受信した属性

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

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

属性	属性番号	構文、タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	86	文字列	シングル	アクセスリスト属性の両方が、Firepower Threat Defense 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（Firepower Threat Defense デバイスに入るトラフィック）または発信（Firepower Threat Defense 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	Firepower Threat Defense デバイスで定義されたネットワークオブジェクトの名前。RA VPN へのクライアント接続のアドレスプールとして使用されるサブネットを識別します。[Objects] ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザーがログインしたときに表示されるバナー。
Banner2	36	文字列	シングル	ユーザーがログインするときに表示されるバナーの 2 番目の部分。Banner2 は Banner1 に付加されます。
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。RA VPN の [Group Policy] ページでグループポリシーを作成する必要があります。次の形式のいずれかを使用できます。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名;
Simultaneous-Logins	2	整数	シングル	ユーザーが確立を許可されている個別の同時接続数。0 ～ 2147483647。

属性	属性番号	構文、タイプ	シングルまたはマルチ値	説明または値
VLAN	140	整数	シングル	ユーザーの接続を制限する VLAN。0 ～ 4094。Firepower Threat Defense デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

二要素認証

RA VPNの二要素認証を設定できます。二要素認証を使用する場合、ユーザーはユーザー名と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サーバーとの関係がプライマリ認証ソースに関連付けられている点です。Duo LDAPは例外で、Duo LDAP サーバーをセカンダリ認証ソースとして設定します。

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サーバーまたはADサーバー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。

- Firewall 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、ユーザーはRSA RADIUSサーバーで設定されているユーザー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 サーバーを使用することが一般的です。2 番目の RADIUS サーバーを認証サーバーとして設定し、必要に応じてアカウンティング サーバーとしても設定します。

- RSA サーバーを、直接統合をサポートする RADIUS または AD サーバーと統合し、プライマリ認証ソースとして非 RSA RADIUS または AD サーバーを使用するように RA VPN を設定します。この場合、RADIUS/ADサーバーはRSA-SDIを使用して、クライアントと RSA サーバー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、ユーザーは非 RSA RADIUS または AD サーバーで設定されているユーザー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 サーバーを認証サーバーとして設定し、必要に応じてアカウンティング サーバーとしても設定します。

RADIUS を使用した Duo 二要素認証

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

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

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

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

- *Duo-passcode*。*my-password*,**12345** など
- **push**。たとえば、*my-password*,**push** など。**push** は、ユーザーによるインストールと登録が完了している Duo モバイルアプリに認証をプッシュ送信するように Duo に指示する場合に使用します。
- **sms**。たとえば、*my-password*,**sms** など。**sms** は、ユーザーのモバイルデバイスにパスコードの新しいバッチと SMS メッセージを送信するように Duo に指示する場合に使用します。**sms** を使用すると、ユーザーの認証試行は失敗します。ユーザーは再認証し、2 番目の要素として新しいパスコードを入力する必要があります。
- **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。

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

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 サーバーとともに、セカンダリ認証ソースとして Duo LDAP サーバーを使用できます。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。

Firepower Threat Defense 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 サーバー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ー名は表示されず、これらのユーザーに対してアクセス制御ルールを作成することはできません。

このアプローチを使用する場合は、RADIUS/AD サーバーと Duo LDAP サーバーの両方で設定されているユーザー名を使用して認証する必要があります。AnyConnect Client 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 （49 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 を設定する前に、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。デバイスを登録するとき、エクスポート制御機能が有効になっている Smart Software Managerのアカウントを使用して登録する必要があります。また、評価ライセンスを使用して機能を設定することはできません。

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：AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only。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、Firewall 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 ライセンスの有効化または無効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、FDM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 AnyConnect Client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。

- デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager アカウントによってエクスポートを制御する必要があります。リモート アクセス VPN を設定するには、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、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。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 ライセンスの有効化または無効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 （任意）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、リモートユーザー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 （任意） 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するユーザ 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 サーバー グループ：プライマリまたはセカンダリ認証ソースとして。認可およびアカウンティングにも。「RADIUS サーバー 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 ユーザーの設定」を参照してください。
- Duo LDAP サーバー：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 サーバーをプライマリ 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 サーバー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 （49 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 サーバー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 （28 ページ）

グループポリシーは、ユーザーに関連する属性を定義します。グループメンバーシップに基づいて、リソースへの差分アクセスを提供するためにグループポリシーを設定することができます。または、すべての接続でデフォルトポリシーを使用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 によるトラフィックの許可 （16 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）。

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 （36 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ー情報またはトラフィック照合用のユーザー情報を取得するには、アイデンティティ ポリシーを有効にする必要があります。

クライアント プロファイルの設定およびアップロード

AnyConnect Clientプロファイルは、AnyConnect Clientソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーがAnyConnect Client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、AnyConnect Client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AnyConnect Clientに表示させるには、VPNプロファイルのサーバーリストに、Firewall 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。

AnyConnect Clientのプロファイルに加えて、必要に応じてAnyConnect Client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、Firewall Device Managerは、AnyConnect Clientプロファイルの作成のみをサポートしています。ただし、Firewall 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、Firewall 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。

次に、オブジェクト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について説明します。オブジェクトリストに表示される**[新規AnyConnectクライアントプロファイルの作成（Create New AnyConnect Client Profile）]**リンクをクリックして、AnyConnect Client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。

- AnyConnect Client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AnyConnect Client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AnyConnect Client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 **[AnyConnectクライアントプロファイル（AnyConnect 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、AnyConnect Client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 AnyConnect Client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。

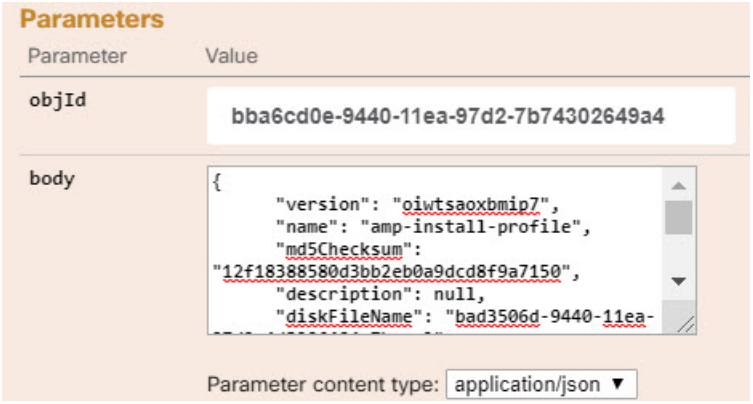

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
```

```
      "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 によるトラフィックの許可

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

- **sysopt connection permit-vpn** コマンドを設定します。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、外部ユーザーがリモート アクセス VPN アドレス プール内の IP アドレス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 トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザーが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

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 （36 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、AnyConnect Clientを使用して VPN 接続を確立します。

Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。必要に応じて、クライアン

トソフトウェアをインストールし、接続を完了します。「AnyConnect Client 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、グループ URL も試してください。

ステップ 2 デバイス CLI にログインします（CLI（コマンドライン インターフェイス）へのログインを参照）。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 AnyConnect Client 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 AnyConnect Client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、ユーザーの認証に使用される AAA サーバーと証明書、ユーザーの IP アドレスを割り当てるためのアドレス プール、およびさまざまなユーザー向け属性を定義するグループ ポリシーを定義します。

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

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（Connection Profiles）] 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ー指向属性を定義します。RA VPN のグループ ポリシーの設定 （28 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、ユーザー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 AnyConnect Client 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（Connection Profiles）] 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。例、MainOffice。IP アドレスは名前として使用できません。

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

- [グループエイリアス（Group Alias）]、[グループURL（Group URL）]：エイリアスには特定の接続プロファイルの代替名または URL を含めることができます。VPN ユーザーは、Firepower Threat Defense デバイスへの接続時に、AnyConnect Client クライアントの接続リストでエイリアス名を選択できます。接続プロファイル名はグループのエイリアスとして自動的に追加されます。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。ユーザーがグループ URL を使用して接続すると、システムはその URL に一致する接続プロファイルを自動的に使用します。この URL は、AnyConnect Client クライアントをまだインストールしていないクライアントによって使用されます。

  グループエイリアスと URL を必要な数だけ追加します。これらのエイリアスと URL は、デバイスで定義されているすべての接続プロファイルで一意である必要があります。グループ URL は **https://** で始まる必要があります。

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

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

これらのオプションにより、リモートアクセス VPN 接続を有効にするための、デバイスへのユーザー認証方法が決定されます。最も簡単なアプローチは、AAA のみを使用し、AD レルムを選択するか、または LocalIdentitySource を使用する方法です。[認証タイプ（Authentication Type）] として次のアプローチを使用できます。

- [AAAのみ（AAA Only）]：ユーザー名とパスワードに基づいてユーザーを認証および認可します。詳細は、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ーを認証します。詳細は、接続プロファイルのための証明書認証の設定 （26 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）]：ユーザー名/パスワードと、クライアント デバイス アイデンティティ証明書の両方を使用します。
- [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 （27 ページ）」を参照してください。

ステップ 7 [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、トンネル確立後のユーザー接続の期間を設定します。システムには、DfltGrpPolicy という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

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 （28 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 グローバル設定を行います。

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。安全な VPN 接続を完了するには、クライアントがこの証明書を承認する必要があります。まだ証明書がない場合、ドロップダウンリストの [新規内部証明書の作成（Create New Internal Certificate）] をクリックします。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）]：リモート アクセス VPN 接続を確立するときにユーザーが接続するインターフェイス。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ー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の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、クライアント プロファイルが作成されます。

（注）
ユーザーは、クライアントによって VPN で使用される DNS サーバーが、この名前から外部インターフェイスの IP アドレスを解決でききるようにする責任があります。関連する DNS サーバーに FQDN を追加します。

- [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 Firewall 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 Firewall 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、ユーザーは 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、VPN フィルタ ACL および AAA サーバーからダウンロードされた認証 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、外部ユーザーがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングし、ネットワークにアクセスするおそれがあります。この理由は、アドレスプールに内部リソースへのアクセスを許可するアクセスコントロールルールを作成する必要があるためです。アクセスコントロールルールを使用する場合は、送信元 IP アドレスだけではなく、ユーザーの仕様を使用してアクセスを制御することを検討してください。

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

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

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 ユーザーがアクセスする内部ネットワークのインターフェイスを選択します。これらのインターフェイスに対して NAT ルールが作成されます。
- [内部ネットワーク（Inside Networks）]：リモート ユーザーがアクセスする内部ネットワークを表すネットワーク オブジェクトを選択します。ネットワーク リストには、サポートしているアドレス プールと同じ IP タイプを含める必要があります。

- **[AnyConnectパッケージ（AnyConnect Packages）]**：RA VPN 接続でサポートする AnyConnect Client 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。エンドポイントに適切なパッケージがインストールされていない場合、ユーザーは、ユーザー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求められます。

ステップ 11 [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、AnyConnect Client 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手順をクリップボードにコピーし、ユーザーに配布します。

ステップ 13 [終了（Finish）] をクリックします。

次のタスク

リモート アクセス VPN によるトラフィックの許可 （16 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、許可、およびアカウンティング（AAA） サーバーは、ユーザー名とパスワードを使用して、ユーザーのリモートアクセス VPN へのアクセスを許可するかどうかを判断します。RADIUS サーバを使用する場合は、認証されたユーザー間で許可レベルを区別して、保護され

たリソースへの差別化されたアクセスを提供できます。使用状況を追跡するためにRADIUSアカウンティングサービスを使用することもできます。

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

プライマリ アイデンティティ ソースのオプション

- [ユーザー認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：リモート ユーザーの認証に使用されるプライマリ アイデンティティ ソース。VPN 接続を完了するには、エンド ユーザがこのソースか任意のフォールバック ソースで定義されている必要があります。次のいずれかを選択します。
  - Active Directory（AD）のアイデンティ レルム。必要なレルムがまだ存在していない場合は、[新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックします。
  - RADIUS サーバーグループ。
  - LocalIdentitySource（ローカル ユーザ 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 サーバー。ただし、これは、Duo LDAP を使用した二要素認証の設定方法（49 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、ユーザー ID 情報は取得されません。ダッシュボードにユーザー情報が表示されず、ユーザー ベースのアクセス制御ルールを作成することもできません。
  - SAML サーバー。SAML サーバーを使用する場合は、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 を認可サーバーとして使用できますが、認証が不要になるようにRADIUS サーバー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 サーバーが認可情報を提供するようにします。
- [フォールバックローカルアイデンティティソース（Fallback Local Identity Source）]：プライマリ ソースが外部サーバーの場合、プライマリ サーバーが使用できない場合のフォールバックとして LocalIdentitySource を選択できます。フォールバック ソースとしてローカル データベースを使用する場合は、必ず外部サーバで定義したものと同じローカル ユーザ名/パスワードを定義します。

[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。次のオプションを有効にすると、ユーザー名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバーが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。

- [ユーザー名からアイデンティティソースサーバーを削除（Strip Identity Source Server from Username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からアイデンティティソース名を削除するかどうか。たとえば、このオプションを選択してユーザーがユーザー名として domain\username を入力すると、ドメインがユーザー名から取り除かれ、認証用に AAA サーバーに送信されます。デフォルトでは、このオプションはオフになっています。
- [ユーザー名からグループを削除（Strip Group from username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からグループを削除するかどうか。このオプションは、username@domain 形式で指定された名前に適用されます。選択すると、domain と @ 記号が削除されます。デフォルトでは、このオプションはオフになっています。

セカンダリ アイデンティティ ソース

- [ユーザー認証用のセカンダリアイデンティティソース（Secondary Identity Source for User Authentication）]：オプションの 2 番目のアイデンティティ ソースです。ユーザーがプライマリ ソースで正常に認証されると、セカンダリ ソースでの認証が求められます。AD レルム、RADIUS サーバーグループ、Duo LDAP サーバー、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ーの場合、セカンダリサーバーが使用できない場合のフォールバックとして LocalIdentitySource を選択できます。フォールバックソースとしてローカルデータベースを使用する場合は、必ずセカンダリ外部サーバーで定義したものと同じローカルユーザー名/パスワードを定義します。
  - [セカンダリログインにプライマリユーザー名を使用（Use Primary Username for Secondary Login）]：デフォルトでは、セカンダリ アイデンティティ ソースを使用する場合、セカンダリ ソースに対してユーザー名とパスワードの両方が求められます。このオプションを選択すると、システムはセカンダリパスワードの入力のみを求め、プライマリ アイデンティティ ソースに対して認証されたものと同じユーザー名をセカンダリ ソースに対して使用します。プライマリとセカンダリの両方のアイデンティティソースで同じユーザー名を設定する場合は、このオプションを選択します。
  - [セッションサーバーのユーザー名（Username for Session Server）]：認証に成功すると、ユーザー名はイベントと統計ダッシュボードに表示され、ユーザーベースまたはグループベースの SSL 復号化およびアクセス制御ルールに一致するものを判断するために使用され、アカウンティングに使用されます。2 つの認証ソースを使用しているため、ユーザーアイデンティティとして、プライマリまたはセカンダリのどちらのユーザー名を使用するのかシステムに通知する必要があります。デフォルトでは、プライマリ名が使用されます。
  - [パスワードタイプ（Password Type）]：セカンダリ サーバーのパスワードを取得する方法。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、[ユーザーログインウィンドウの証明書からユーザー名を事前入力（Prefill username from certificate on user login window）] と [ログインウィンドウでユーザー名を非表示にする（Hide username in login window）] の両方を選択します。デフォルトは [プロンプト（Prompt）] で、ユーザーはパスワードの入力が求められることを意味します。

プライマリサーバーへのユーザー認証時に入力したパスワードを自動的に使用するには、[プライマリアイデンティティソースのパスワード（Primary Identity Source Password）] を選択します。

すべてのユーザーに同じパスワードを使用するには [共通パスワード（Common Password）] を選択し、[共通パスワード（Common Password）] フィールドにそのパスワードを入力します。

その他のオプション

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

  認証の完了後、認可によって、認証済みの各ユーザーが使用できるサービスおよびコマンドが制御されます。認可は、ユーザーが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザーに対して同じアクセス権を提供します。認可のための 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ー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 サーバーから取得した場合、RADIUS 属性は、グループポリシー属性をオーバーライドすることに注意してください。

- [アカウンティングサーバー（Accounting Server）]：（オプション）リモートアクセス VPN セッションへのアカウンティングに使用する RADIUS サーバーグループ。

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

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。

クライアント証明書を使用していても、セカンダリ アイデンティティ ソース、フォールバック ソース、および認証およびアカウンティングサーバーを引き続き設定できます。これらは

AAA オプションです。詳細については 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。

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

- [証明書のユーザー名（Username from Certificate）]：次のいずれかを選択します。
  - [マップ固有フィールド（Map Specific Field）]：証明書の要素を [プライマリフィールド（Primary Field）] および [セカンダリフィールド（Secondary Field）] の順番で使用します。デフォルトはCN（共通名）と OU（組織単位）です。組織に適したオプションを選択します。これらのフィールドを組み合わせてユーザー名が提供され、このユーザー名がイベント、ダッシュボード、さらにSSL復号とアクセス制御ルールでのマッチング目的に使用されます。
  - [DN（識別名）全体をユーザー名として使用（Use entire DN (distinguished name) as username）]：システムが自動的に DN フィールドからユーザー名を導出します。
- [詳細オプション（Advanced options）]：[詳細（Advanced）] リンクをクリックし、次のオプションを設定します。
  - [ユーザーログインウィンドウの証明書からユーザー名を事前入力（Prefill username from certificate on user login window）]：ユーザーに認証を要求するときに、取得したユーザー名をユーザー名フィールドに入力するかどうか。
  - [ログインウィンドウでユーザー名を非表示にする（Hide username in login window）]：[事前入力（Prefill）] オプションを選択すると、ユーザー名を非表示にできます。これは、ユーザーがパスワードプロンプトでユーザー名を編集できないことを意味します。

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 サーバー、DHCP サーバー、グループポリシーで設定されている IP アドレスプール、または接続プロファイルで設定された IP アドレスプールによって提供されます。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 Firewall 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 サーバーで、そのオブジェクト名を使用してユーザーの 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 サーバーを指定します。
- [DHCP]：まず、1 つ以上の IPv4 アドレス範囲を持つ RA VPN の DHCP サーバーを設定します（DHCP を使用して IPv6 プールを設定することはできません）。次に、DHCP サー

バーの IP アドレスを使用してホスト ネットワーク オブジェクトを作成します。その後、このオブジェクトは接続プロファイルの [DHCPサーバー（DHCP Servers）] 属性で選択できます。最大 10 台の DHCP サーバーを設定できます。

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

- [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ー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、ユーザー接続の条件を設定するグループポリシーが使用されます。グループ ポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

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

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 （29 ページ）
  - セッション設定属性 （30 ページ）
  - アドレス割り当て属性 （30 ページ）
  - スプリット トンネリング属性 （31 ページ）
  - AnyConnect Client 属性 （32 ページ）
  - トラフィック フィルタ属性 （34 ページ）
  - Windows ブラウザ プロキシ属性 （35 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サーバー（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 サーバーを定義する DNS サーバーグループを選択します。必要なグループがまだ定義されていない場合は、[DNSグループの作成（Create DNS Group）] をクリックしてすぐに作成します。
- [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。AnyConnect Clientは、 部分的な HTML をサポートしています。リモート ユーザーへバナーが適切に表示されることを確認するには、
 タグを使用して改行を示します。
- [デフォルトドメイン（Default Domain）]：RA VPN内のユーザーのデフォルトドメインの名前。例、example.com。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。
- **[AnyConnectクライアントプロファイル（AnyConnect Client Profiles）]**：[+] をクリックし、このグループに使用する AnyConnect Client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 AnyConnect Client プロファイルエディタを使用してこれらのプロファイルを作成します。スタンドアロン AnyConnect プロファイルエディタは、software.cisco.com からダウンロードしてインストールできます。クライアントプロファイルを選択しない場合、AnyConnect Client クライアントはすべてのオプションにデフォルト値を使用します。このリストの項目は、プロファイル自体ではなく AnyConnect Client プロファイル オブジェクトです。新しいプロファイルを作成（およびアップロード）するには、ドロップダウンリストで**[新規AnyConnectクライアントプロファイルの作成（Create New AnyConnect Client Profile）]** をクリックします。

AnyConnect Clientプロファイルに加えて、AMP イネーブラなどの AnyConnect Client 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）]：ユーザーがログアウト、再接続せずに VPN に接続したままにできる最大時間（分）で、1 ～ 4473924 または空白で指定します。デフォルトは無制限（空白）ですが、その場合でもアイドル タイムアウトは適用されます。
- [接続時間のアラート間隔（Connection Time Alert Interval）]：最大接続時間を指定した場合、アラート間隔は、次回の自動切断についてユーザーに警告を表示する、最大時間に達するまでの時間を定義します。ユーザーは、接続を終了し、再接続してタイマーを再起動することを選択できます。デフォルトは 1 分です。1 ～ 30 分を指定できます。
- [アイドルタイム（Idle Time）]：VPN 接続が自動的に閉じられる前にアイドル状態になる時間（分）で、1 ～ 35791394 で指定します。指定した時間、接続で通信アクティビティがない場合、システムは接続を停止します。デフォルトは 30 分です。
- [アイドル時間のアラート間隔（Idle Time Alert Interval）]：アイドル セッションが原因の次回の自動切断について、ユーザーに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。
- [ユーザーあたり同時ログイン（Simultaneous Logins Per User）]：ユーザーに許可する同時接続の最大数。デフォルトは 3 です。1 ～ 2147483647 個の接続を指定できます。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プールからアドレスが割り当てられます。

- [DHCPスコープ（DHCP Scope）]：接続プロファイルのアドレス プールに DHCP サーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じ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 サーバーはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

  スコープを指定するには、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 サーバーは、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（Create New Network）] 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。ユーザーが RA VPN 接続を行うと、ユーザー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 サーバーに他の DNS 要求を送信することを許可しながら、セキュアな接続を介していくつかの 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が、すべての DNS 要求をグループで定義された DNS サーバーに保護された接続を介して送信する場合は、このオプションを選択します。
  - [指定したドメインのみをトンネル経由で送信（Send only specified domains over tunnel）]：保護された DNS サーバーが特定のドメインのアドレスだけを解決するようにしたい場合は、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。例：example.com, example1.com。内部 DNS サーバーが内部ドメインの名前を解決し、外部 DNS サーバーが他のすべてのインターネットトラフィックを処理するようにする場合は、このオプションを使用します。

AnyConnect Client 属性

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

SSL 設定

- [Datagram Transport Layer Security（DTLS）の有効化（Enable Datagram Transport Layer Security (DTLS)）]：AnyConnect Client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 AnyConnect Client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、各ユーザー セッションのメモリ要件と CPU 使用率も高めます。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（None）] を選択して、キーの再生成を無効にします。キーの再生成を有効にするには、新しいトンネルを作成するたびに [新しいトンネル（New Tunnel）] を選択します（[既存のトンネル（Existing Tunnel）] オプションは、[新しいトンネル（New Tunnel）] と同じアクションになります）。キーの再生成を有効にする場合は、キーの再生成間隔も設定します。デフォルトは 4 分です。間隔は、4 ～ 10080 分（1 週間）の範囲で設定できます。

接続の設定

- [DF（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。

  AnyConnect Clientがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが AnyConnect Client 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 AnyConnect Client 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]：AnyConnect Clientによって確立されたSSL VPN接続の最大伝送ユニット（MTU）サイズ。デフォルトは 1406 バイトで、範囲は 576 ー 1462 バイトです。
- **[AnyConnectとVPNゲートウェイ間のキープアライブメッセージ（Keepalive Messages Between AnyConnect and VPN Gateway）]**：トンネルでのデータの送受信にピアを使用できることを示すために、ピア間でキープアライブメッセージを交換するかどうかを指定します。キープアライブ メッセージは、設定された間隔で送信されます。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。
- [ゲートウェイ側の間隔でのDPD（DPD on Gateway Side Interval）]、[クライアント側の間隔でのDPD（DPD on Client Side Interval）]：ピアが応答しなくなったときに VPN ゲートウェイまたは VPN クライアントによる迅速な検出を確実に実行するには、Dead Peer Detection（DPD）を有効にします。ゲートウェイまたはクライアント DPD を個別に有効にすることができます。DPD メッセージのデフォルトの送信間隔は 30 秒です。間隔は、5～3600 秒にすることができます。

トラフィック フィルタ属性

グループポリシーのトラフィックフィルタ属性は、グループに割り当てられているユーザーに適用する制限を定義します。アクセス コントロール ポリシー ルールを作成する代わりにこれらの属性を使用することで、ホストまたはサブネット アドレスとプロトコル、または VLAN に基づいて、特定のリソースに RA VPN ユーザーを制限することができます。

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

- [アクセスリストのフィルタ（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（Create Extended Access List）] 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する場合は、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 ブラウザプロキシ属性は、ユーザーのブラウザで定義されたプロキシが動作しているかどうか、およびその動作方法を判断します。

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

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

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ー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 Firewall 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 AnyConnect Clientをダウンロードするため、外部 IP アドレスに対し AnyConnect Client 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、ユーザーが 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。

AnyConnect Client 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、AnyConnect Client 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 AnyConnect Client 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 AnyConnect Client 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。

AnyConnect Client 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、AnyConnect Clientをダウンロードしてインストールできても、AnyConnect Client 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、ユーザーが正しいユーザー名とパスワードを入力しており、ユーザー名が認証サーバーで正しく定義されていることを確認してください。認証サーバー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） 認証サーバー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。詳細は、リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバーを使用する方法 （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 サーバーを更新し、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 AnyConnect Client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 AnyConnect Client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、Firewall 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. AnyConnect Client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、Firewall Threat Defense デバイスはトラフィックを返していません。Firewall 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（Firewall Threat Defense デバイスが認識しない）ことを確認します。

3. Firewall 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、Firepower Threat Defense 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 サーバーを使用する場合は、認可変更ポリシーの適用を設定できます。

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 Firepower Threat Defense 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、Firepower Threat Defense 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、エンドポイントが条件に準拠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ーの権限を昇格したりできます。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 Firepower Threat Defense 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、AnyConnect Clientを使用して、Firepower Threat Defense デバイスとの RA VPN セッションを開始します。
2. Firepower Threat Defense デバイスはそのユーザーの RADIUS Access-Request メッセージを ISE サーバーに送信します。
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対して設定されている認証ポリシーにユーザーを一致させます。このポリシーは、ISE が RADIUS Access-Accept の応答で Firepower Threat Defense 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、Firepower Threat Defense デバイスで設定されている拡張 ACL の名前です。この ACL は、どのユーザー トラフィックを ISE サーバーにリダイレクトすべきか（HTTP トラフィック）を定義します。次に例を示します。

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

   - **url-redirect=***url*：トラフィックのリダイレクト先 URL。次に例を示します。

     ```
     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サーバーに到達できることを確認します。

4. Firepower Threat Defense デバイスは 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、Firepower Threat Defense 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。Firepower Threat Defense 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、Firepower Threat Defense 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、Firepower Threat Defense 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、必要なポスチャ コンプライアンス モジュールがクライアントにあるかどうかを判断し、必要に応じてユーザー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. Firepower Threat Defense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 Firepower Threat Defense 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、AnyConnect Client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。AnyConnect Client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。

Firewall 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 サーバーで設定されます。ただし、Firepower Threat Defense 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、この設定の Firepower Threat Defense 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 サーバー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 サーバーに送信されるトラフィックは送信しません。リダイレクト ACL の例を次に示します。

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

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

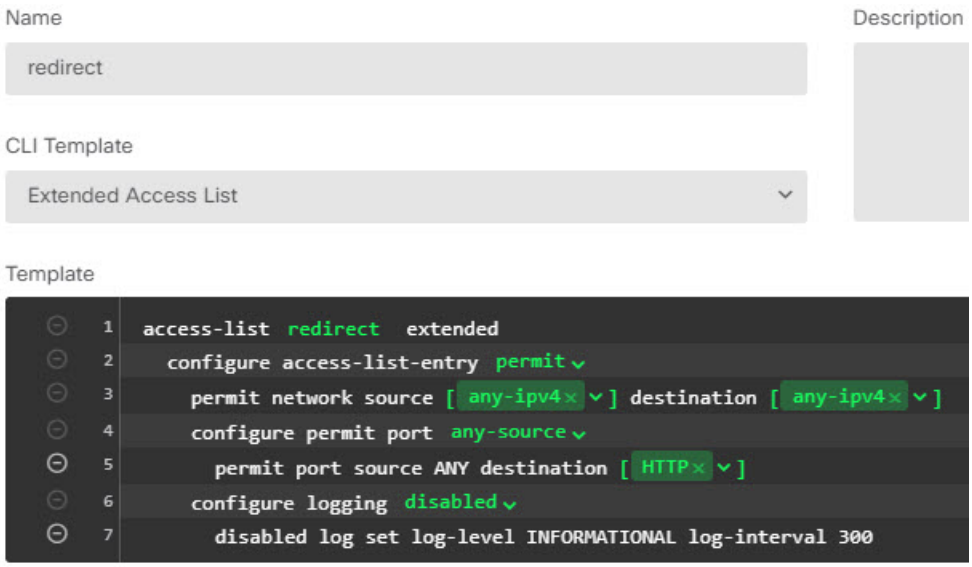
リダイレクト ACL では、permit および deny アクションによって、ACL に一致するトラフィックが特定されることに注意してください（permit は一致、deny は不一致）。トラフィックは実際にはドロップされず、拒否されたトラフィックは ISE にリダイレクトされません。

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

a) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（Smart CLI）]** > **[オブジェクト（Objects）]** 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 サーバーへのトラフィックはリダイレクトされないようにするために、他の ACE を追加することもできます。最初に、それらのサーバーの IP アドレスを保持するホスト ネットワーク オブジェクトを作成する必要があります。

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

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 サーバーとサーバー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（Objects）]** > **[アイデンティティ ソース（Identity Sources）]** を選択します。

b) **[+]** > **[RADIUSサーバー（RADIUS Server）]** をクリックします。

c) サーバーの名前と、ISE RADIUS サーバーのホスト名または IP アドレス、認証ポート、およびサーバー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。

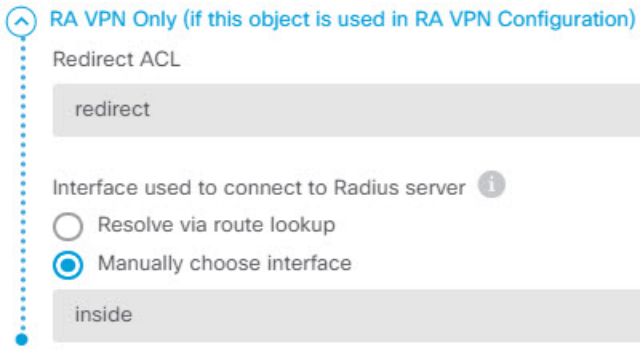
d) [RA VPN専用（RA VPN Only）] リンクをクリックし、次のオプションを設定します。

- [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サーバー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、サーバー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。

  サーバーが管理アドレスと同じネットワーク上にある場合（これは診断インターフェイスを選択することを意味します）、診断インターフェイスで IP アドレスを設定する必要もあります。管理 IP アドレスがあるだけでは不十分です。**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** に移動し、管理 IP アドレスと同じサブネット上にある診断インターフェイスで IP アドレスを設定します。

  Firewall 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ーオブジェクトを保存します。

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

f) **[+]** > **[RADIUSサーバーグループ（RADIUS Server Group）]** をクリックします。

g) サーバー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 サーバー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 サーバーを使用してユーザーを認証するように RADIUS サーバーが設定されている場合は、この RADIUS サーバーと組み合わせて使用される AD サーバーを指定する [RADIUSサーバー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サーバー（RADIUS Server）] の下で [+] をクリックし、RA VPN 用に作成したサーバーオブジェクトを選択します。

k) [OK] をクリックしてサーバー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 サーバー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）、[ユーザー認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]、[認可（Authorization）]、および [アカウンティング（Accounting）] オプションでサーバー グループを選択します。

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 サーバーに 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 サーバーで設定されます。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 ステータスを決定します。Firepower Threat Defense デバイスは基本的に、特定のエンドユーザーの処理に関する 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 サーバーでユーザーがすでに設定済みであると想定しています。

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、Firepower Threat Defense 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、Firepower Threat Defense 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、Firepower Threat Defense 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。ユーザーに求められる正確なアクセスを準拠状態に基づいて提供するために、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、Firepower Threat Defense 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 Firepower Threat Defense デバイスに送信します。これにより、RA VPN ユーザー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、準拠ユーザー向けに 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 Firepower Threat Defense デバイスに送信します。デバイスは、これをユーザーセッションに適用します。この DACL は、ユーザーセッションの初期のリダイレクト 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。AnyConnect Client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（Common Tasks）]：[DACL名（DACL Name）] を選択し、非準拠ユーザー向けに 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 Firepower Threat Defense デバイスに送信します。デバイスは、これをユーザーセッションに適用します。この DACL は、ユーザーセッションの初期のリダイレクト 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

個別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 ユーザー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、ユーザー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)）]：AnyConnect Client 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 AnyConnect Client 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 AnyConnect Client 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 AnyConnect Client 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（Policy）] > [クライアントプロビジョニング（Client Provisioning）]** 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 AnyConnect Client 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（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]** 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、ユーザー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（Policy）] > [ポリシーセット（Policy Sets）] > [デフォルト（Default）] > [認証ポリシー（Authorization Policy）]** 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（Administration）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]** 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。ポスチャ再評価を有効にして、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。ユーザーの続行を許可する（接続したまま）、ユーザーをログオフさせる、またはユーザーにシステムの修復を依頼することができます。

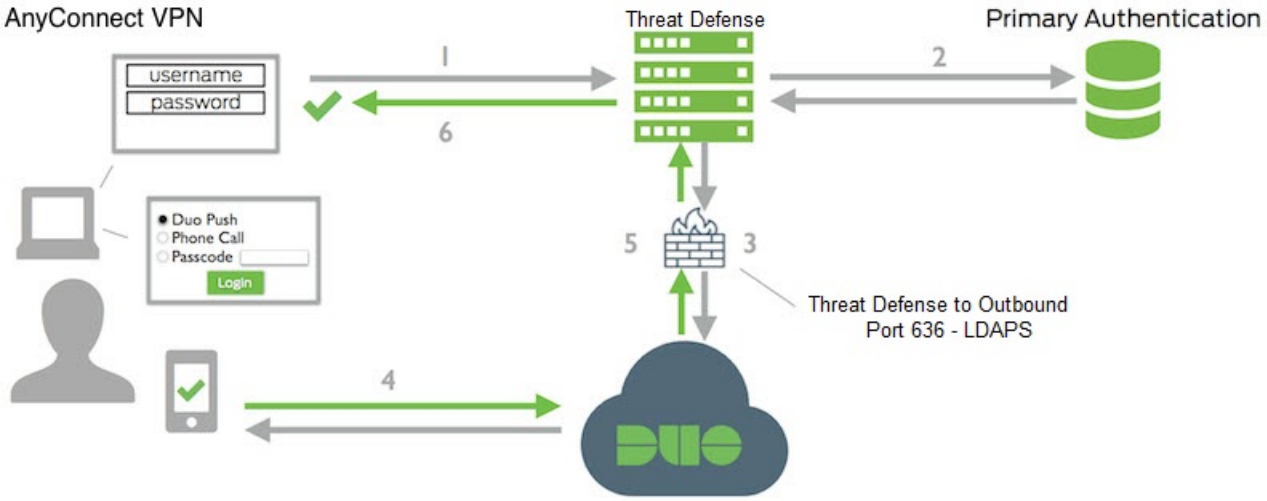
Duo LDAP を使用した二要素認証の設定方法

プライマリソースとしての Microsoft Active Directory（AD）または RADIUS サーバーとともに、セカンダリ認証ソースとして Duo LDAP サーバーを使用できます。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、Firepower Threat Defense と Duo がどのように連携するかを示しています。



次に、システムフローについて説明します。

1. ユーザーは、Firepower Threat Defense 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. Firewall 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、Firepower Threat Defense は Duo LDAP サーバーにセカンダリ認証の要求を送信します。
4. 要求を受けた Duo は、プッシュ構成、パスコード付きのテキストメッセージ、または電話コールによって、ユーザーを個別に認証します。ユーザーはこの認証を正常に完了する必要があります。
5. Duo は Firepower Threat Defense 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、Firepower Threat Defense デバイスは、ユーザーの AnyConnect Client 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、統合鍵、秘密鍵、および API ホスト名を取得します。

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

a) Duo アカウントにサインアップします。
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、統合鍵、秘密鍵、および API ホスト名を取得します。詳細については、Duo 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 サーバーの 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、Firepower Threat Defense API を使用する必要があります。Firewall 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) Firewall 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 サーバー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 サーバー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
- type
- version
- name

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 [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）。
- [name] には、Duo-LDAP-server などのオブジェクトの名前を入力します。
- [description] 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 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。
- [port] には、LDAPS に使用する TCP ポートを入力します。Duo から別のポートを使用するように指示されていない限り、この値は 636 になります。アクセス制御リストで、必ずこのポートを介した Duo LDAP サーバーへのトラフィックを許可してください。
- [timeout] には、Duo サーバーに接続する際のタイムアウトを秒単位で入力します。値は 1 ー 300 秒です。デフォルトは 120 です。デフォルトを使用するには、120 を入力するか、属性行を削除します。
- [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鍵を入力します。この鍵はその後マスクされます。
- [interface] には、Duo LDAP サーバー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）。
- [type] 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、Firewall Device Manager に戻ります。

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

Firewall 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 Firewall Device Manager にアップロードします。

Firewall 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、[全般（General）] タブに、DigiCert High Assurance EV Root CA に発行されたことが示されます。これは、Firewall 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。

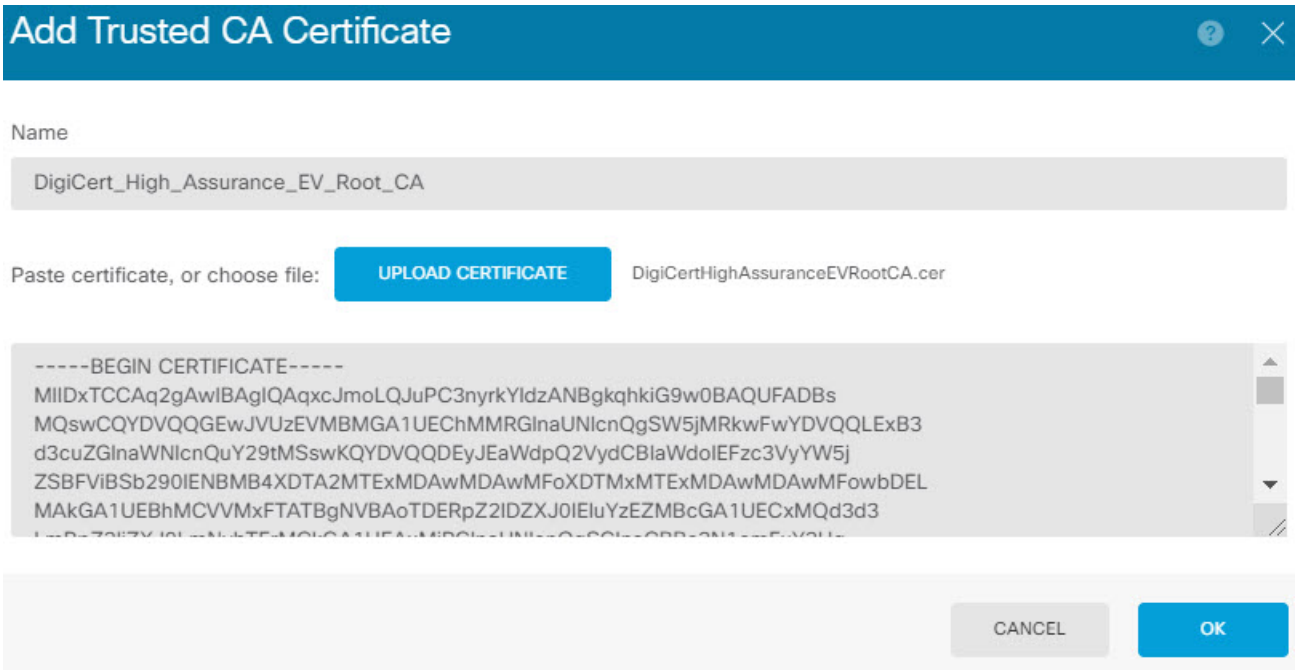
f) ウィザードを使用して、ワークステーションに証明書をダウンロードします。デフォルトの DER 形式を使用してダウンロードします。

g) Firewall 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 AnyConnect Client 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。

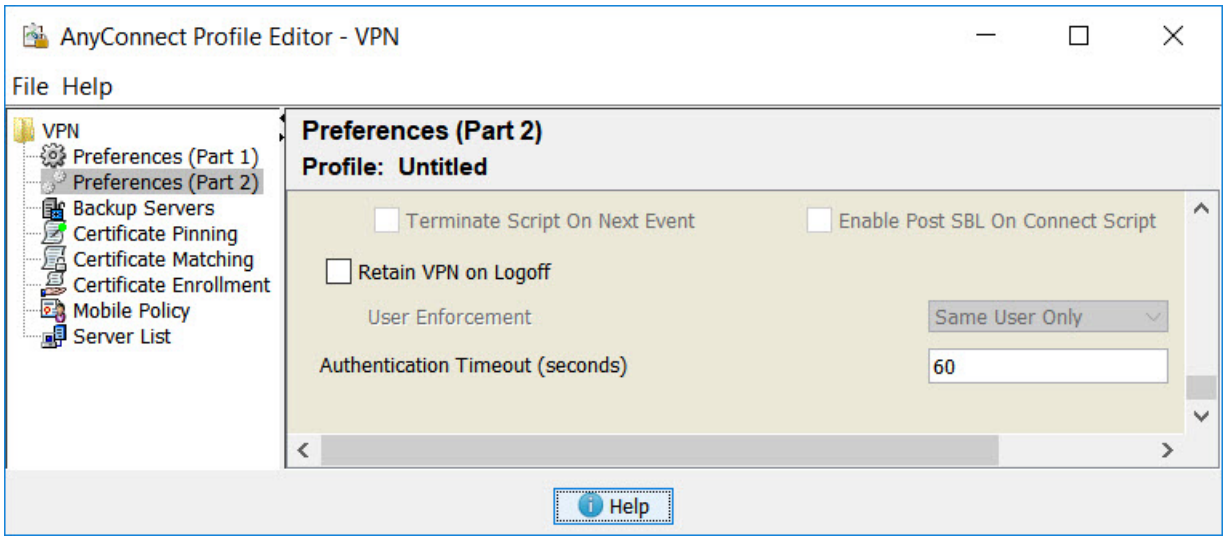
ユーザーが Duo のパスコードを取得し、セカンダリ認証を完了できるように、指定する時間に余裕を持たせる必要があります。60 秒以上を推奨します。

AnyConnect Client 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、Firewall 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) AnyConnect Client プロファイル エディタ パッケージをダウンロードしてインストールします（まだ行っていない場合）。このパッケージは、Cisco Software Center（software.cisco.com）の使用している AnyConnect Client バージョンのフォルダにあります。

b) AnyConnect Client 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。

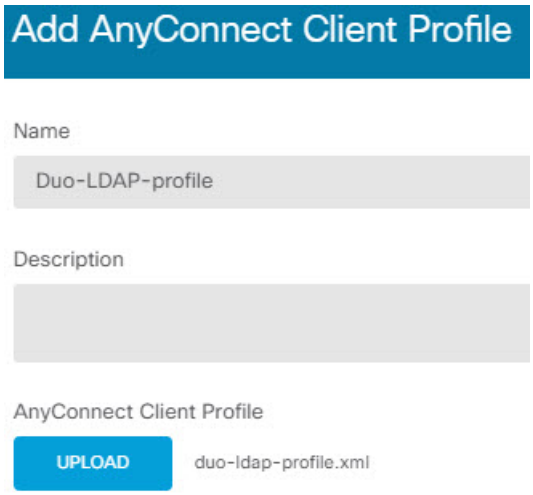
これで、VPN プロファイル エディタ アプリケーションを閉じることができます。

e) Firewall Device Managerで、**[オブジェクト（Objects）]** > **[AnyConnectクライアントプロファイル（AnyConnect 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。



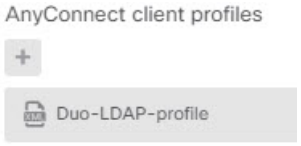
i) [OK] をクリックします。

ステップ 5 グループポリシーを作成し、ポリシーで AnyConnect Client プロファイルを選択します。

ユーザーに割り当てるグループポリシーは、接続のさまざまな側面を制御します。次の手順では、プロファイル XML ファイルをグループに割り当てる方法について説明します。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 （28 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) 目次の [グループポリシー（Group Policies）] を選択します。
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、すべてのユーザーに対して 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（General）] ページで、次のプロパティを設定します。

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

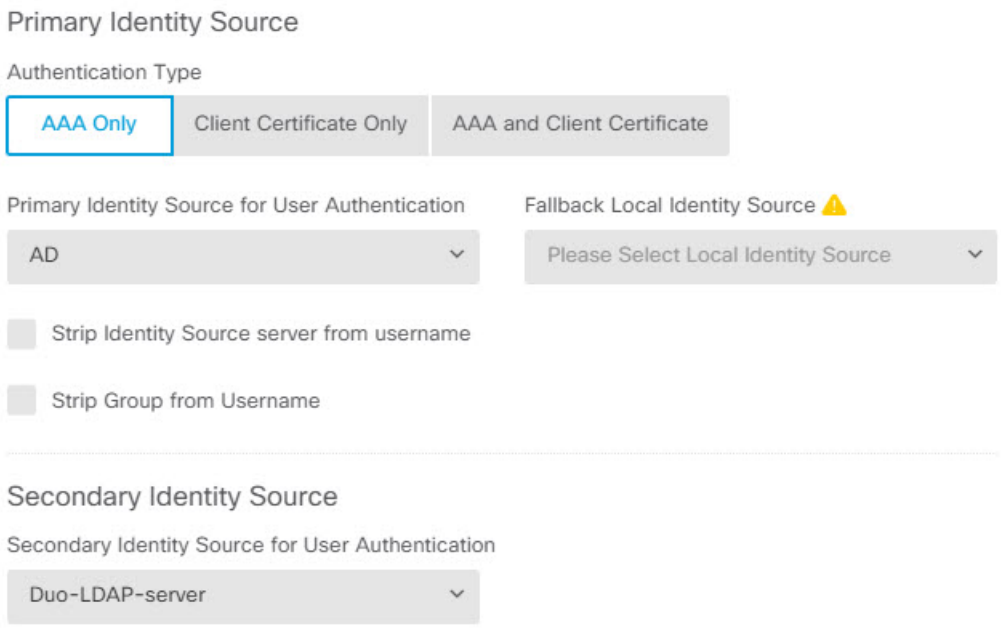
接続プロファイルを設定するには数多くの手順があります。詳細については、RA VPN 接続プロファイルの設定 （19 ページ）を参照してください。次の手順では、Duo-LDAP をセカンダリ認証ソースとして有効にし、AnyConnect Client クライアントプロファイルを適用するための主な変更について説明します。新しい接続プロファイルの場合は、残りの必須フィールドも設定する必要があります。この手順では、既存の接続プロファイルを編集していて、これら 2 つの設定だけ変更する必要があると仮定しています。

a) [RA VPN] ページで、目次の [接続プロファイル（Connection Profiles）] を選択します。
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（Primary Identity Source）] で、次を設定します。

- [認証タイプ（Authentication Type）]：[AAAのみ（AAA Only）] または [AAAとクライアント証明書（AAA and Client Certificate）] のいずれかを選択します。AAA を使用していない場合、二要素認証を設定できません。
- [ユーザー認証のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：プライマリ Active Directory または RADIUS サーバーを選択します。プライマリソースとして Duo-LDAP アイデンティティソースを選択できることに注意してください。ただし、Duo-LDAP は認証サービスのみを提供し、アイデンティティサービスは提供しないため、プライマリ認証ソースとして Duo-LDAP を使用する場

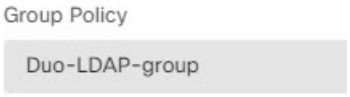
合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザー名は表示されず、これらのユーザーに対してアクセス制御ルールを作成することはできません（必要に応じて、ローカル アイデンティティ ソースへのフォールバックを設定できます）。

- [セカンダリ アイデンティティ ソース（Secondary Identity Source）]：Duo-LDAP のアイデンティティソースを選択します。



d) [Next] をクリックします。

e) [リモートユーザーエクスペリエンス（Remote User Experience）] 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。

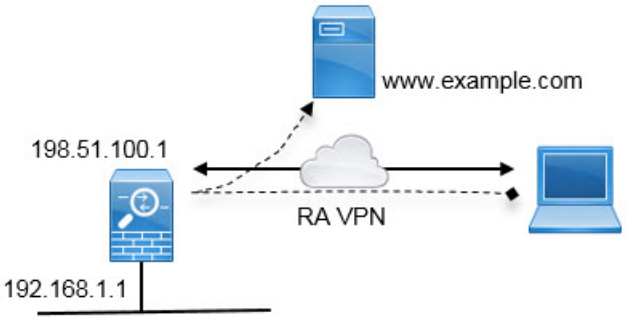
b) [Deploy Now] ボタンをクリックします。

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

外部インターフェイスでリモート アクセス VPN ユーザーにインターネット アクセスを提供する方法（ヘア ピニング）

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

次の図は例を示しています。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、AnyConnect Client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

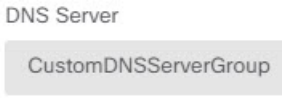
ステップ 1 リモートアクセス VPN 接続を設定します。

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

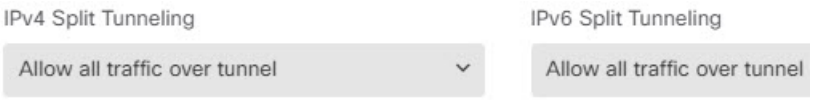
の例では新しいグループポリシーを作成するのではなく、デフォルトグループポリシーを編集します。どちらのアプローチも取ることができます。

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) 目次で [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サーバー（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あるサーバーを定義する DNS サーバー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。



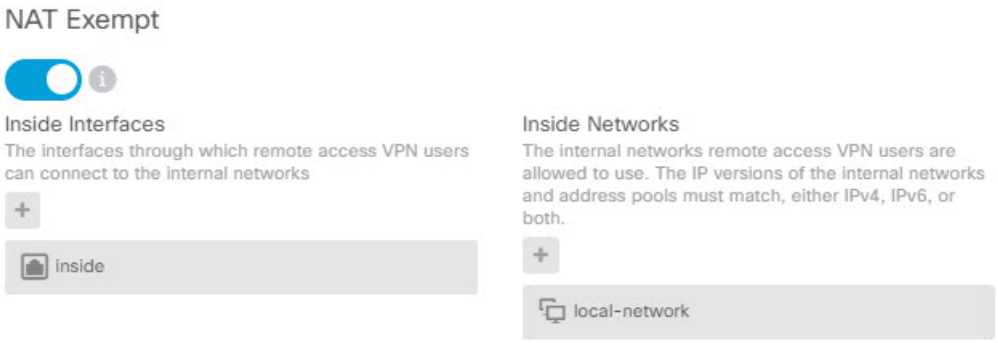
（注）
これは、ヘアピン接続を有効にするための重要な設定です。すべてのトラフィックを VPN ゲートウェイに向かわせる場合、スプリット トンネリングは、リモート クライアントが VPN の外部にあるローカル サイトやインターネット サイトに直接アクセスできるようにするための方法です。

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一つの重要な設定です。

g) （オプション）[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させますが（外部ユーザーがプール内のアドレスをスプーフィングできません）、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送信されたすべての接続を外部 IP アドレス（インターフェイス PAT）のポートに変換するよう NAT ルールを設定します。

デバイスの初期設定を完了すると、InsideOutsideNatRule という名前の NAT ルールが作成されます。このルールは、外部インターフェイス経由でデバイスを抜ける任意のインターフェイスから、インターフェイス PAT を IPv4 トラフィックに充当します。外部インターフェイスは「任意の」送信元インターフェイスに含まれるため、必要なルールは、編集または削除していない限り、すでに存在しています。

次の手順で、必要なルールを作成する方法を説明します。

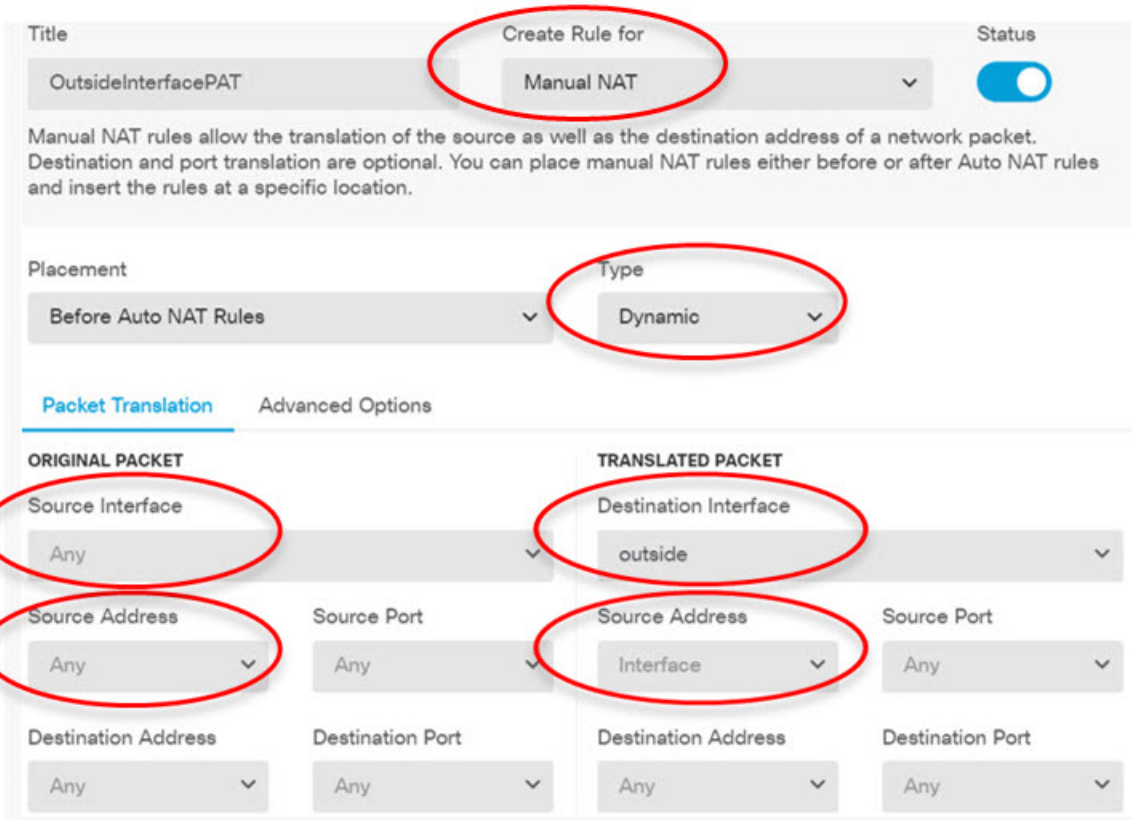
a) **[ポリシー（Policies）]** > **[NAT]** をクリックします。
b) 次のいずれかを実行します。

- InsideOutsideNatRule を編集するには、[アクション（Action）] 列にマウス オーバーし、[編集（edit）] アイコン（）をクリックします。
- ルールを新規作成するには、[+] ボタンをクリックします。

c) 次のプロパティを使用してルールを設定します。

- [タイトル（Title）]：新しいルールのわかりやすい名前をスペースを含めず入力します。たとえば、OutsideInterfacePAT と入力します。
- [ルールの作成先（Create Rule For）]：[手動NAT（Manual NAT）]。
- [配置（Placement）]：[自動NATルールの前（Before Auto NAT Rules）]（デフォルト）。
- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [元のパケット（Original Packet）]：[送信元アドレス（Source Address）] で [任意（Any）] または [any-ipv4] を選択します。[送信元インターフェイス（Source Interface）] で、[任意（Any）]（デフォルト）を選択していることを確認します。[元のパケット（Original Packet）] の他のすべてのオプションは、デフォルトの [任意（Any）] のままにします。
- [変換後のパケット（Translated Packet）]：[宛先インターフェイス （Destination Interface）] で、[外部（outside）] を選択します。[変換後のアドレス（Translated Address）] で、[インターフェイス（Interface）] を選択します。[変換後のパケット（Translated Packet）] の他のすべてのオプションは、デフォルトの [任意（Any）] のままにします。

次の図は、発信元アドレスに [任意（Any）] を選択したシンプルな例を示しています。



d) [OK] をクリックします。

ステップ 3 （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。

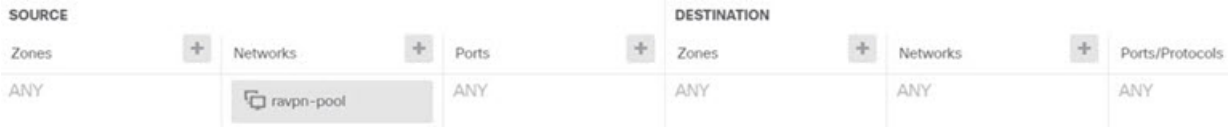
次の例では、アドレスプールから任意の宛先へのトラフィックが許可されます。これは独自の要件に合わせて調整できます。不要なトラフィックを除外するブロック ルールをルールの前に置くことができます。

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

- [順序（Order）]：ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。デフォルトでは、ルールはポリシーの最後に追加

されます。ルールの位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。

- [タイトル（Title）]：スペースを含めずにわかりやすい名前を入力します。例、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）] 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]、および [ユーザー（Users）] タブ：これらのタブではデフォルトの設定（何も選択しない）のままにします。
- [侵入（Intrusion）]、[ファイル（File）] タブ：オプションで、脅威またはマルウェアを検索する侵入またはファイル ポリシーを選択できます。
- [ロギング（Logging）] タブ：オプションで接続のロギングを有効にできます。

d) [OK] をクリックします。

ステップ 4 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) [Deploy Now] ボタンをクリックします。

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

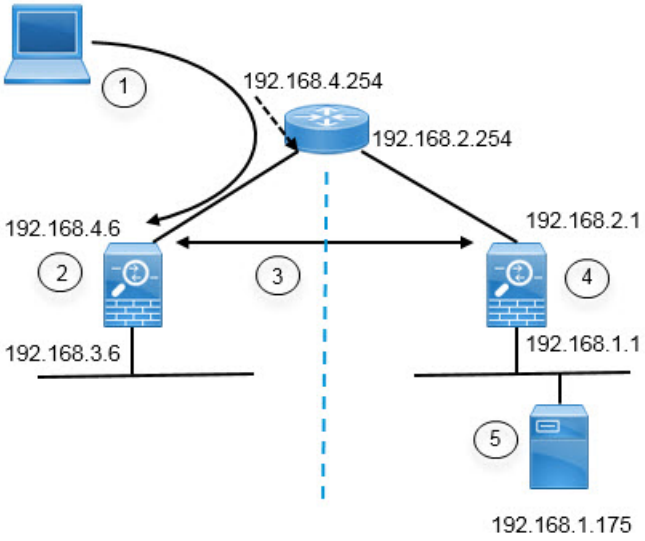
リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバーを使用する方法

モバイル ワーカーと在宅勤務者が内部ネットワークに安全に接続できるリモートアクセスVPNを設定できます。接続のセキュリティは、ユーザー接続を認証して、認可されたユーザーだけがエントリを取得できるようにするディレクトリ サーバーによって異なります。

ディレクトリ サーバーが内部ネットワークではなく外部ネットワーク上にある場合、外部インターフェイスからディレクトリ サーバーを含む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 の設定の 1つのテクニック**：サイト間 VPN 接続の「内部」ネットワーク内、および背後にディレクトリ サーバーが存在するデバイスのリモート ネットワークに、リモート アクセス VPN デバイスの外部インターフェイス アドレスを含める必要があります。詳細については、次の手順を参照してください。

（注） データインターフェイスを仮想管理インターフェイスのゲートウェイとして使用する場合、この設定により、アイデンティティ ポリシー用のディレクトリの使用も可能になります。データインターフェイスを管理ゲートウェイとして使用しない場合は、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ます。

この使用例では、次のネットワーク シナリオを実装します。



図のコールアウト	説明
1	192.168.4.6 に VPN 接続を行うリモート アクセス ホスト。クライアントは 172.18.1.0/24 アドレス プールにあるアドレスを取得します。
2	リモート アクセス VPN をホストするサイト A。
3	サイト A とサイト B の Firepower Threat Defense 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	ディレクトリ サーバーをホストするサイト B。
5	サイト B の内部ネットワークにあるディレクトリ サーバー。

始める前に

この使用例は、デバイスのセットアップ ウィザードを使用して、通常のベースラインの構成を構築していることを前提としています。具体的には次のとおりです。

- inside_zone から outside_zone に移動するトラフィックを許可（または信頼）する Inside_Outside_Rule アクセス コントロール ルールがある。
- inside_zone と outside_zone のセキュリティ ゾーン（それぞれ）に、内部インターフェイスと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に移動す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、インターフェイス PAT 用のルールが複数存在する場合がある。
- 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 アドレスを使用しているが、DHCP を使用してスタティック ルートの動的取得も可能であることを前提としています。この例の場合、次のスタティック ルートを想定しています。
  - 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 サーバーをホストする [サイトB（Site B）] にサイト間 VPN 接続を設定します。

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

b) [+] ボタンをクリックします。

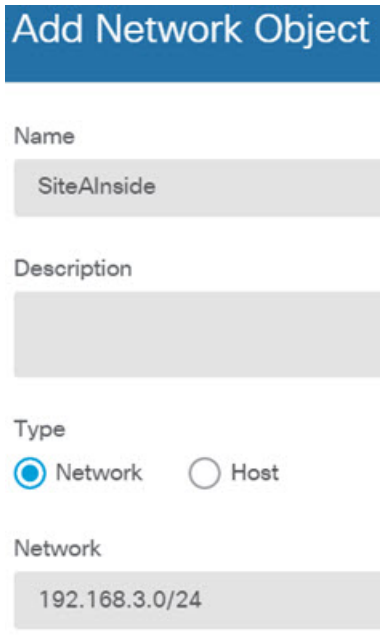
c) [エンドポイントの設定（Endpoint Settings）] に次のオプションを設定します。

- [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 A への接続を示す、SiteA）。
- [ローカルサイト（Local Site）]：これらのオプションでローカル 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）]：[外部（outside）]インターフェイス（図の 192.168.2.1 アドレスが付いているインターフェイス）を選択します。
  - [ローカルネットワーク（Local Network）]：[+] をクリックして、VPN 接続に参加する必要があるローカル 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 サーバーはこのネットワーク上にあるため、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、[新規ネットワークの作成（Create New Network）] をクリックして、192.168.1.0/24 ネッ

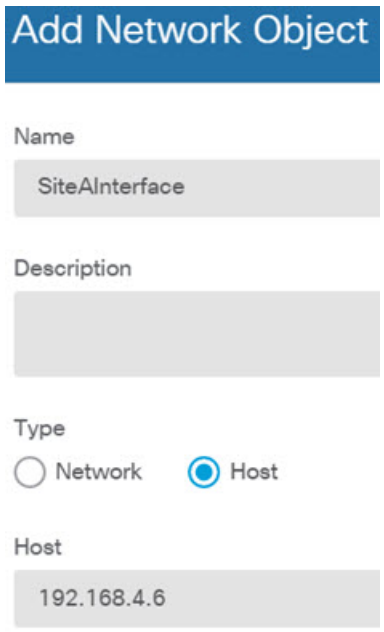
トワークのオブジェクトを設定します。オブジェクトを保存したら、ドロップダウン リストでそのオブジェクトを選択し、[OK] をクリックします。

- [リモートサイト（Remote Site）]：これらのオプションでリモート エンドポイントを定義します。
  - [リモートIPアドレス（Remote IP Address）]：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 アドレスである 192.168.4.6 を入力します。
  - [リモートネットワーク（Remote Network）]：[+] をクリックして、VPN 接続に参加する必要があるリモート ネットワークを特定するネットワーク オブジェクトを選択します。[新規ネットワークの作成（Create New Network）] をクリックして、次のオブジェクトを設定し、リストでそれらのオブジェクトを選択します。

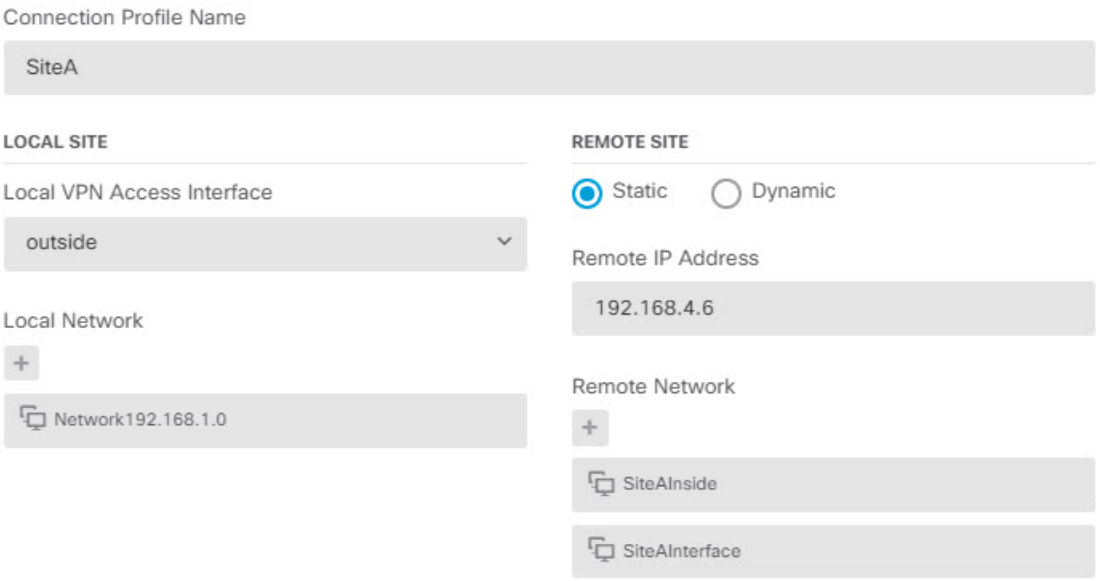
    1. SiteAInside、ネットワーク、192.168.3.0/24。



2. SiteAInterface、ホスト、192.168.4.6。**重要ポイント：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 接続用のリモート ネットワークの一部として含めて、当該インターフェイスでホストされている RA VPN でディレクトリ サーバーを使用可能にする必要があります。**



終了すると、エンドポイントの設定は次のようになります。



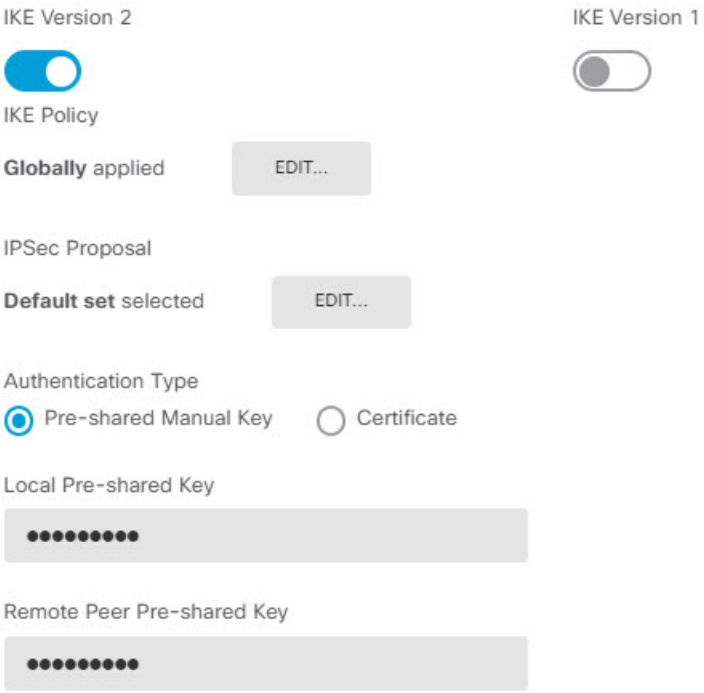
d) [Next] をクリックします。

e) VPN のプライバシー設定を定義します。

この使用例は、強力な暗号化の使用を許可する輸出管理機能を承認していることを前提としています。これらの例の設定は、お客様のニーズとライセンス コンプライアンスに合わせて調整してください。

- [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（[IKEバージョン2（IKE Version 2）] は有効で、[IKEバージョン1（IKE Version 1）] は無効）のままにします。
- [IKEポリシー（IKE Policy）]：[編集（Edit）]をクリックして、[AES-GCM-NULL-SHA] および [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プロポーザルの選択（Select IPSec Proposals）] ダイアログボックスで [+] をクリックし、[デフォルトに設定（Set Default）] をクリックしてデフォルトの AES-GCM プロポーザルを選択します。
- [ローカルの事前共有キー（Local Preshared Key）]、[リモートピアの事前共有キー（Remote Peer Preshared Key）]：このデバイスおよび VPN 接続用のリモート デバイスに定義されているキーを入力します。これらのキーは IKEv2 では異なることがあります。このキーには 1 ～ 127 の英数字を指定できます。**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を選択します。この例では [内部（inside）]インターフェイス。通常、サイト間 VPN トンネル内のトラフィックの IP アドレスは変換しません。このオプションは、ローカル ネットワークが 1 つのルーテッドインターフェイス（ブリッジグループ メンバーではない）の背後にある場合にのみ機能します。ローカル ネットワークが複数のルーテッドインターフェイスまたは 1 つ以上のブリッジ グループのメンバーの背後にある場合、NAT 免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法の詳細については、NAT からのサイト間 VPN トラフィックの除外を参照してください。
- [Perfect Forward Secrecy用のDiffie-Helman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固有のセッション 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決定します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイント デバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。オプションの説明については、使用する Diffie-Hellman 係数グループの決定を参照してください。

この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) サマリーを確認し、[終了（Finish）] をクリックします。

サマリー情報がクリップボードにコピーされます。この情報はドキュメントに貼り付けて、リモート ピアの設定、またはピアの設定責任者に送信するために使用できます。

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 のデバイスがサイト間 VPN 接続の一端をホストできるようになりました。

ステップ 2 [サイトB（Site B）]デバイスからログアウトして、[サイトA（Site 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（Site A）] にサイト間 VPN 接続を設定します。

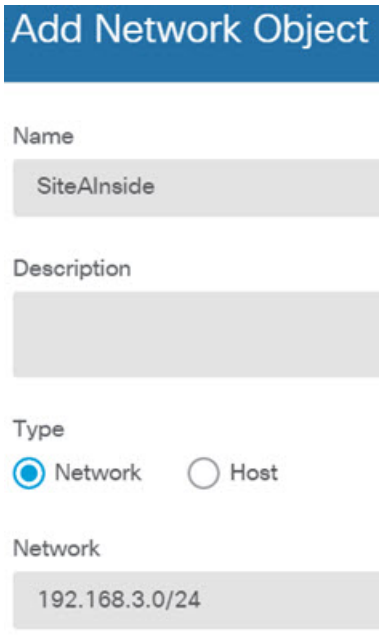
a) [デバイス（Device）] をクリックし、[サイト間VPN（Site-to-Site VPN）] グループで [設定の表示（View Configuration）] をクリックします。

b) [+] ボタンをクリックします。

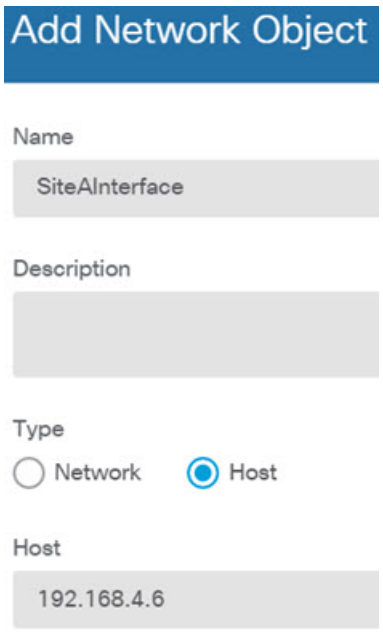
c) [エンドポイントの設定（Endpoint Settings）] に次のオプションを設定します。

- [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）。
- [ローカルサイト（Local Site）]：これらのオプションでローカル 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）]：[外部（outside）]インターフェイス（図内 192.168.4.6 アドレスが付いているインターフェイス）を選択します。
  - [ローカルネットワーク（Local Network）]：[+] をクリックして、VPN 接続に参加する必要があるローカル 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。[新規ネットワークの作成（Create New Network）] をクリックして、次のオブジェクトを設定し、リストでそ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、ネットワーク、192.168.3.0/24。



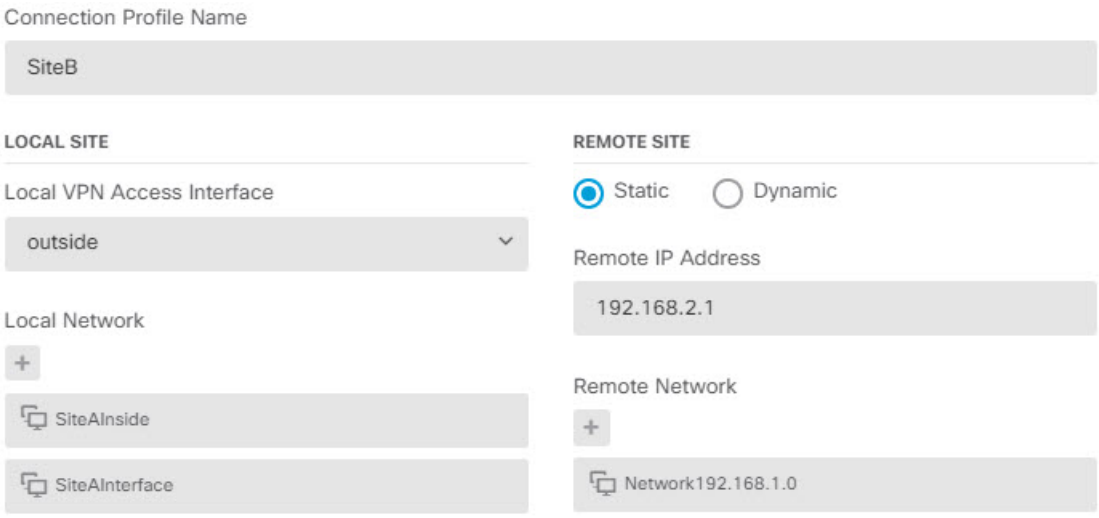
2. SiteAInterface、ホスト、192.168.4.6。**重要ポイント：リモート アクセス VPN 接続ポイントのアドレスをサイト間 VPN 接続用の内部ネットワークの一部として含めて、当該インターフェイスでホストされている RA VPN でリモート ネットワーク上のディレクトリ サーバーを使用可能にする必要があります。**



- [リモートサイト（Remote Site）]：これらのオプションでリモート エンドポイントを定義します。

- [リモートIPアドレス（Remote IP Address）]：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 アドレスである 192.168.2.1 を入力します。
- [リモートネットワーク（Remote Network）]：[+] をクリックして、VPN 接続に参加する必要があるリモート ネットワークを特定する（ディレクトリ サーバーを含んでいる）ネットワーク オブジェクトを選択します。[新規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ら、ドロップダウンリストで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、エンドポイントの設定は次のようになります。ローカルおよびリモート ネットワークは、サイト B の設定と比べると反転している点に注意してください。これは、ポイントツーポイント接続の両端の通常の外観を示しています。

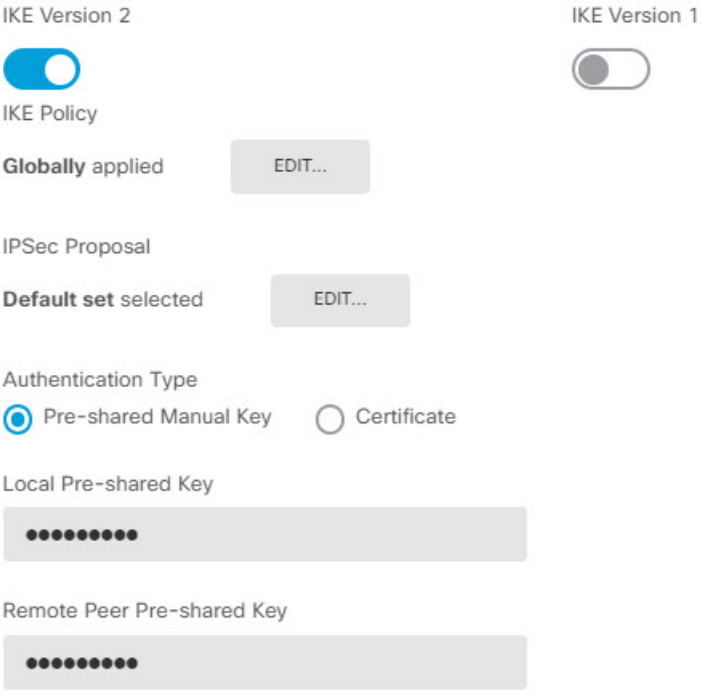


d) [Next] をクリックします。

e) VPN のプライバシー設定を定義します。

サイト B 接続の場合と同じ IKE バージョン、ポリシー、および IPsec プロポーザルと、同じ事前共有キーを設定します。**ただし、必ず、ローカル事前共有キーとリモート事前共有キーを逆にしてください。**

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を選択します。この例では [内部（inside）]インターフェイス。通常、サイト間 VPN トンネル内のトラフィックの IP アドレスは変換しません。このオプションは、ローカルネットワークが 1 つのルーテッドインターフェイス（ブリッジグループ メンバーではない）の背後にある場合にのみ機能します。ローカル ネットワークが複数のルーテッドインターフェイスまたは 1 つ以上のブリッジ グループのメンバーの背後にある場合、NAT 免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法の詳細については、NAT からのサイト間 VPN トラフィックの除外を参照してください。
- [Perfect Forward Secrecy用のDiffie-Helmanグループ（Diffie-Helman Group for Perfect Forward Secrecy）]：[グループ19（Group 19）] を選択します。

このオプションは次のようになります。

g) [次へ（Next）] をクリックします。
h) サマリーを確認し、[終了（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 のデバイスがサイト間 VPN 接続のもう一端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ですでに設定されているため、2 台のデバイスは VPN 接続をネゴシエートする必要があります。

デバイスの CLI にログインし、ディレクトリ サーバーに ping することで、接続を確認できます。**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（Site A）] のディレクトリ サーバーを設定します。[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。例、AD。

- [タイプ（Type）]：ディレクトリ サーバのタイプ。サポートされるタイプは Active Directory のみで、このフィールドを変更することはできません。
- [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）。

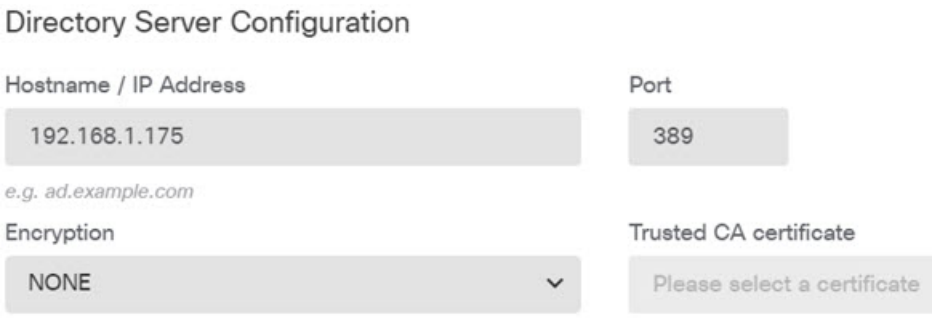
  （注）
  この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=adminisntrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [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。例、cn=users,dc=example,dc=com。ベース DN の検索の詳細については、ディレクトリ ベースの 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がある完全修飾 Active Directory ドメイン名。例、example.com。

d) ディレクトリ サーバのプロパティを設定します。

- [ホスト名またはIPアドレス（Hostname/IP Address）]：ディレクトリ サーバのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。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。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。この例では、389 のままにします。

- [暗号化（Encryption）]：ユーザーおよびグループ情報のダウンロードに暗号化された接続を使用します。デフォルトは[なし（None）]で、ユーザーおよび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、LDAP over SSL である [LDAPS] 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）]：暗号化方式を選択する場合、認証局（CA）の証明書をアップロードして、システムとディレクトリ サーバ間の信頼できる接続を有効にします。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IPアドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 192.168.1.175 を使用し、証明書では ad.example.com を使用している場合、接続は失敗します。



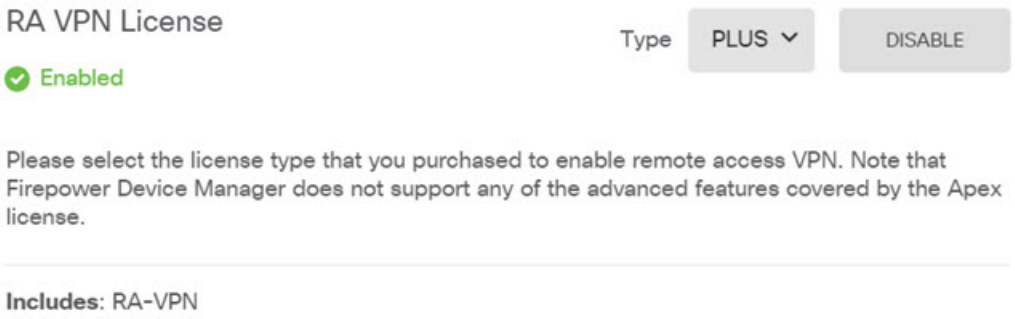
e) [テスト（Test）] ボタンをクリックして、システムがサーバーに接続できることを確認します。

サーバー アクセスには異なるプロセスが使用されるため、アイデンティティ ポリシーには使用できるが、リモート アクセス VPN には使用できないなど、あるタイプの使用においては接続が機能するが別のタイプでは機能しないことを示すエラーが表示されることがあります。サーバーに到達できない場合は、正しい IP アドレスとホスト名を指定していること、DNS サーバーに当該ホスト名のエントリなどが設定されていることを確認します。また、サイト間 VPN 接続が機能していること、サイト A の外部インターフェイス アドレスを VPN に含めていること、および NAT がディレクトリ サーバーのトラフィックを変換していないことを確認します。サーバーのスタティック ルートを設定する必要がある場合もあります。

f) [OK] をクリックします。

ステップ 5 **[デバイス（Device）]** > **[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。

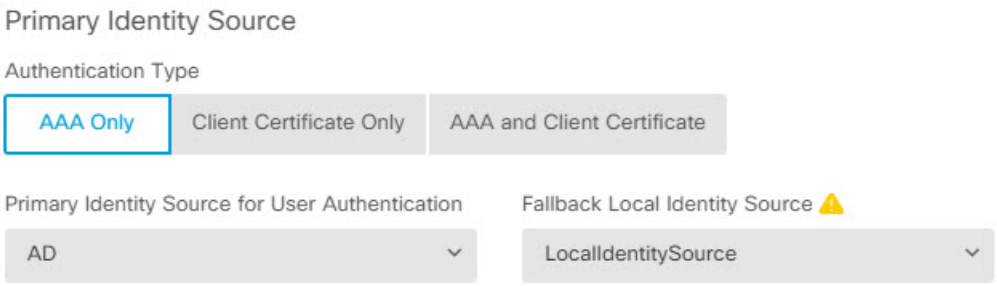


ステップ 6 サイト A のリモートアクセス VPN を設定します。

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。アドレス プールを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設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。

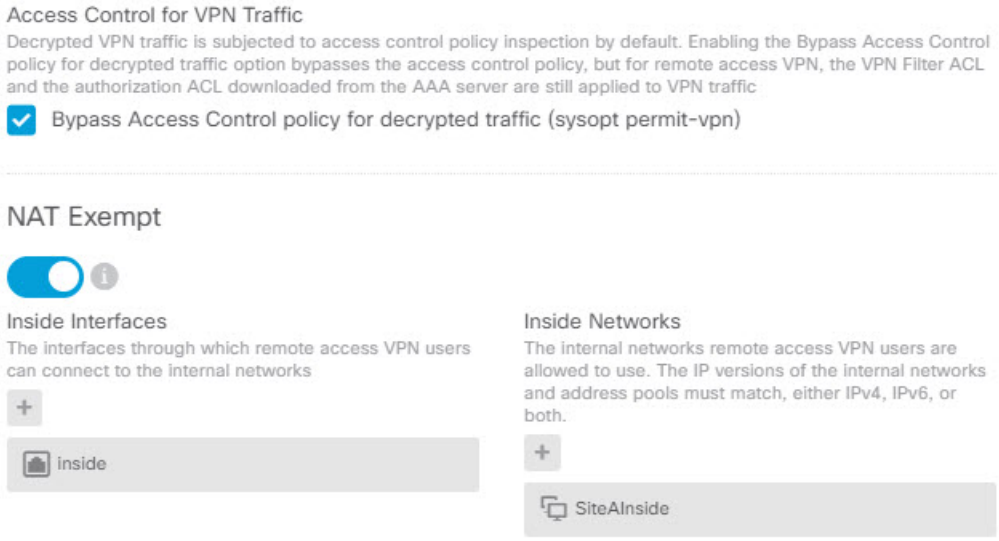
e) [次へ（Next）] をクリックし、適切なグループポリシーを選択します。

選択したポリシーに関する要約情報を確認します。DNS サーバー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、内部ネットワークのリモートユーザーがアクセスする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）]：SiteAInside ネットワーク オブジェクトを選択します。これらは、内部ネットワークのリモートユーザーがアクセスするオブジェクト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 AnyConnect Client 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、AnyConnect Client 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（Finish）] 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 AnyConnect Client 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。これらのユーザーに制限を適用する場合は、デフォルトグループポリシーを編集して、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）。

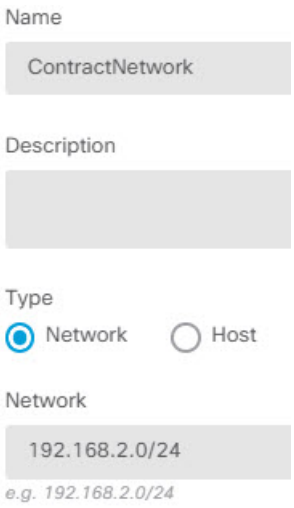
手順

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

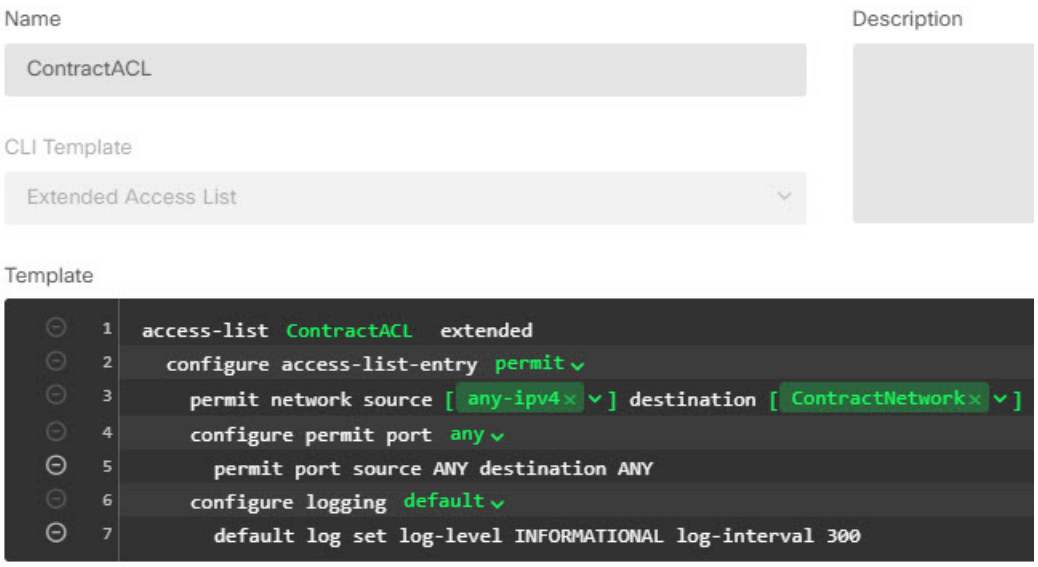
たとえば、オブジェクトに ContractNetwork という名前を付けます。オブジェクトは、次のようになります。



b) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（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。

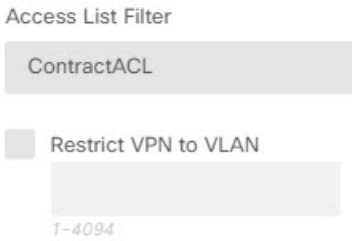
この ACL は、次に変更を展開するときに設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

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、グループポリシーの DNS サーバー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（Traffic Filters）] 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。

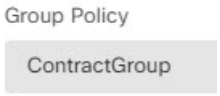
ステップ 3 コントラクタの接続プロファイルを設定します。

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。

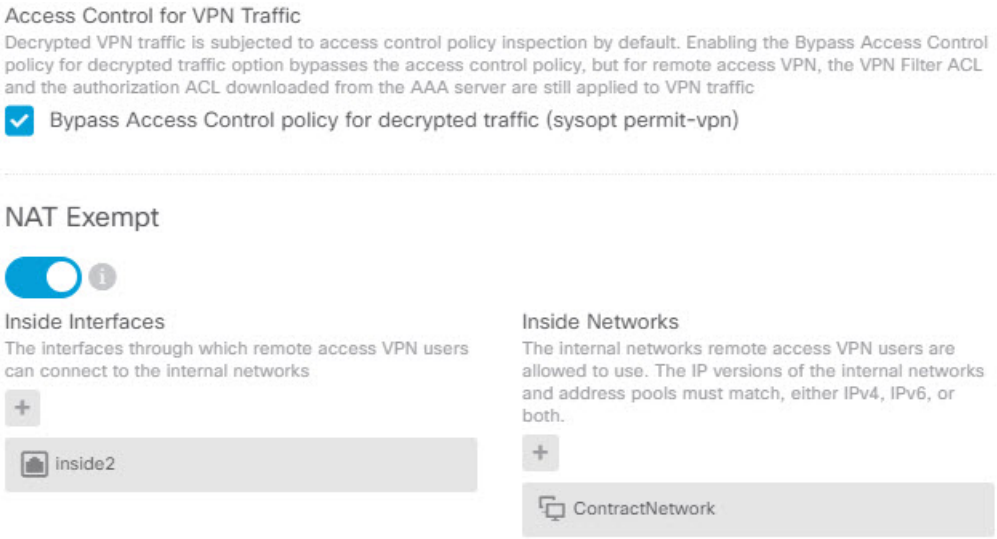
d) 請負業者用に設定されているグループポリシーを選択し、[次へ（Next）] をクリックします。



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、内部ネットワークのリモートユーザーがアクセスする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、内部ネットワークのリモートユーザーがアクセスするオブジェクト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 AnyConnect Client 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、AnyConnect Client 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。

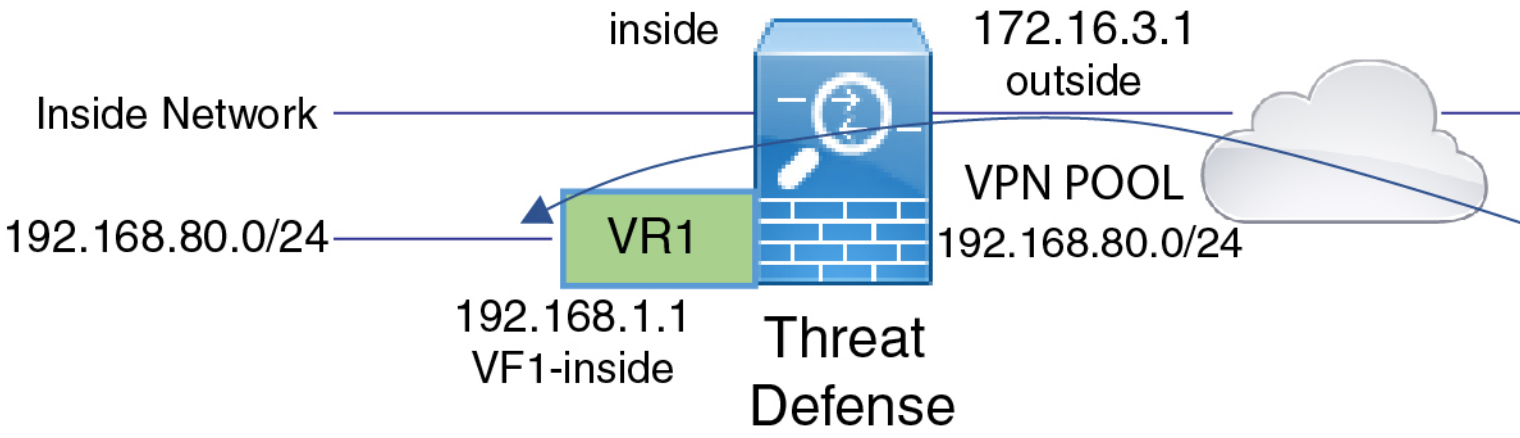
h) [終了（Finish）] をクリックします。

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 ユーザー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。

次の例を考えてみます。RA VPN ユーザーが 172.16.3.1 の外部インターフェイスに接続するとします。このユーザーには 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、このユーザーは、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 ユーザー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。

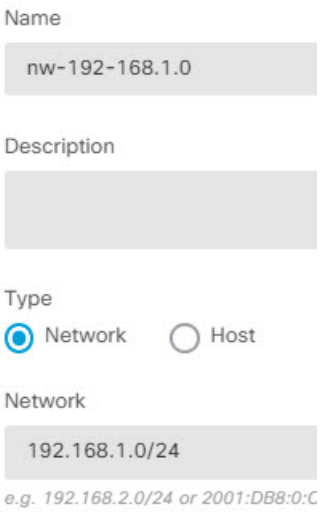
このルートにより、VPN プール内の IP アドレスが割り当てられた AnyConnect Clientは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできるようになります。

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。

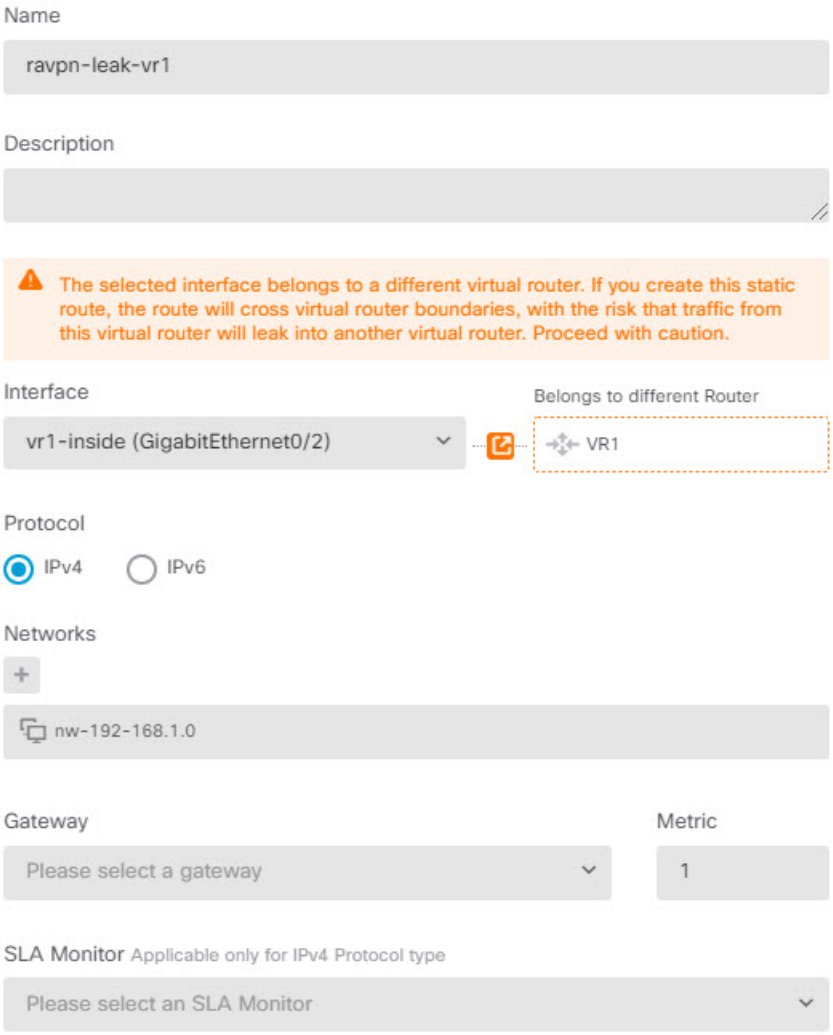
c) グローバルルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [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。

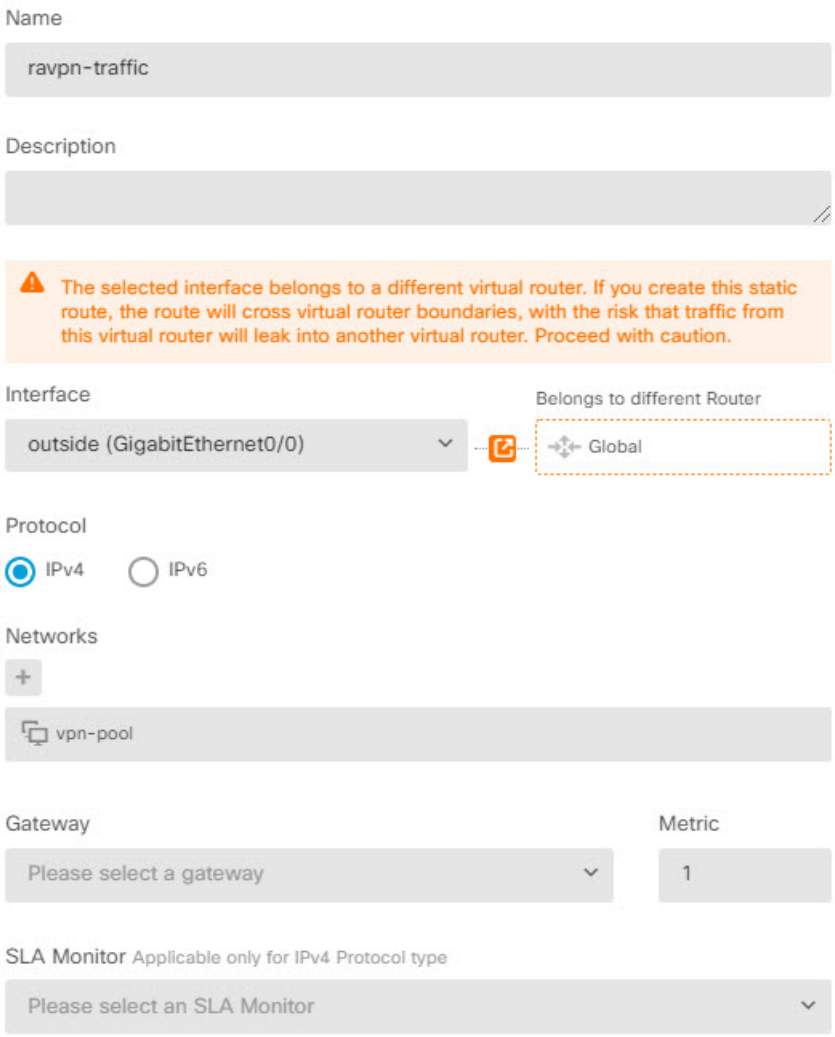
ステップ 2 VR1 からグローバル仮想ルータへのルートリークを設定します。

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 AnyConnect Client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。

AnyConnect Client 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 AnyConnect Client 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 AnyConnect Secure Mobility Client Administrator Guide*』の AnyConnect Client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、Firewall 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 サーバーを使用できます。これらのファイルから画像を取得するための URL には、サーバーのセットアップで必要なパスとユーザー名/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 Firewall 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 Firewall 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 のユーザー 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 Firewall 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 サーバーの 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、AnyConnect Client 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では、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、引き続き診断CLIを使用していると想定すると、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、ユーザー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。次に例を示します。

```
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。

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。