



一般的な VPN 設定

- システム オプション (2 ページ)
- 最大 VPN セッション数の設定 (3 ページ)
- DTLS の設定 (4 ページ)
- DNS サーバー グループの設定 (5 ページ)
- 暗号化コアのプールの設定 (5 ページ)
- SSL VPN 接続用のクライアント アドレス指定 (6 ページ)
- グループ ポリシー (8 ページ)
- 接続プロファイル (54 ページ)
- IKEv1 接続プロファイル (75 ページ)
- **IKEv2 接続プロファイル** (81 ページ)
- IPsec または SSL VPN 接続プロファイルへの証明書のマッピング (83 ページ)
- Site-to-Site 接続プロファイル (87 ページ)
- Cisco Secure Client イメージの AnyConnect VPN モジュール (96 ページ)
- AnyConnect クライアント外部ブラウザ SAML パッケージ (98 ページ)
- AnyConnect クライアントVPN 接続の設定 (99 ページ)
- AnyConnect クライアント HostScan (107 ページ)
- HostScan/Secure Firewall ポスチャのインストールまたはアップグレード (108 ページ)
- HostScan/Secure Firewall ポスチャのアンインストール (110 ページ)
- グループポリシーへの AnyConnect クライアント機能モジュールの割り当て (110 ページ)
- HostScan/Secure Firewall ポスチャ関連資料 (112 ページ)
- Secure Client ソリューション (112 ページ)
- AnyConnect クライアントのカスタマイズとローカリゼーション (114 ページ)
- AnyConnect クライアント カスタム属性 (118 ページ)
- IPsec VPN クライアント ソフトウェア (120 ページ)
- Zone Labs Integrity Server (120 ページ)
- ISE ポリシーの適用 (122 ページ)

システムオプション

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [System Options] ペイン（または [Configuration] > [Site-to-Site VPN] > [Advanced] > [System Options] を使用して到達）を使用すると、ASA 上の IPsec セッションと VPN セッションに固有の機能を設定できます。

- [Limit maximum number of active IPsec VPN sessions] : アクティブな IPsec VPN セッションの最大数の制限をイネーブルまたはディセーブルにします。範囲は、ハードウェアプラットフォームとソフトウェア ライセンスによって異なります。
- [Maximum IPsec Sessions] : アクティブな IPsec VPN セッションの最大許可数を指定します。このフィールドは、上記のチェックボックスをオンにして、アクティブな IPsec VPN セッションの最大数を制限した場合にだけアクティブになります。
- [L2TP Tunnel Keep-alive Timeout] : キープアライブ メッセージの頻度を秒単位で指定します。範囲は 10 ~ 300 秒です。デフォルトは 60 秒です。これは、Network (Client) Access 専用の高度なシステム オプションです。
- VPN トンネルの確立時に、既存のフローを再分類します。
- [Preserve stateful VPN flows when the tunnel drops] : ネットワーク拡張モード (NEM) での IPsec トンネルフローの保持をイネーブルまたはディセーブルにします。永続的な IPsec トンネルフロー機能をイネーブルにすると、[Timeout] ダイアログボックスでトンネルが再作成される限り、セキュリティアプライアンスがステート情報にアクセスできるため、データは正常にフローを続行します。このオプションは、デフォルトで無効です。



(注) トンネル TCP フローはドロップされないため、クリーンアップは TCP タイムアウトに依存します。ただし、特定のトンネルフローのタイムアウトがディセーブルになっている場合、手動または他の方法（ピアからの TCP RST など）によってクリアされるまで、そのフローはシステム内で保持されます。

- [IPsec Security Association Lifetime] : セキュリティアソシエーション (SA) の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
- [Time] : 時 (hh) 、分 (mm) 、および秒 (ss) 単位で SA のライフタイムを指定します。
- [Traffic Volume] : キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロードデータのキロバイト数を入力します。または [unlimited] をオンにします。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。

- [Enable PMTU (Path Maximum Transmission Unit) Aging] : 管理者が PMTU のエージングをイネーブルにすることができます。
 - [Interval to Reset PMTU of an SA (Security Association)] : PMTU 値が元の値にリセットされる秒数を入力します。
- [Enable inbound IPSec sessions to bypass interface access-lists]. [Group policy and per-user authorization ACLs still apply to the traffic] : ASA は、VPN トラフィックが ASA インターフェイスで終了することをデフォルトで許可するので、IKE または ESP (またはその他のタイプの VPN パケット) をアクセスルールで許可する必要はありません。このオプションをオンにしている場合は、復号化された VPN パケットのローカル IP アドレスに対するアクセスルールは不要です。VPN トンネルは VPN セキュリティメカニズムを使用して正常に終端されたので、この機能によって、構成が簡略化され、セキュリティリスクを負うことなく、デバイスのパフォーマンスが最大化されます。(グループポリシーおよびユーザー単位の許可 ACL は、引き続きトラフィックに適用されます)。

このオプションをオフにすることにより、アクセスルールをローカル IP アドレスに適用することを強制的に適用できます。アクセスルールはローカル IP アドレスに適用され、VPN パケットが復号化される前に使用されていた元のクライアント IP アドレスには適用されません。
- [Permit communication between VPN peers connected to the same interface] : この機能をイネーブルまたはディセーブルにします。

同じインターフェイスを介して着信クライアント VPN トラフィックを暗号化せずに、または暗号化してリダイレクトすることもできます。同じインターフェイスを介して VPN トラフィックを暗号化せずに送信する場合は、そのインターフェイスに対する NAT をイネーブルにし、プライベート IP アドレスをパブリックにルーティング可能なアドレスに変換する必要があります (ただし、ローカル IP アドレスプールですでにパブリック IP アドレスを使用している場合は除きます)。
- [Compression Settings] : 圧縮をイネーブルにする機能 (WebVPN および SSL VPN クライアント) を指定します。圧縮はデフォルトでイネーブルになっています。

最大 VPN セッション数の設定

VPN セッションまたは AnyConnect クライアント VPN セッションで許可される最大数を指定するには、次の手順を実行します。

手順

- ステップ 1 [Configuration] > [Remote Access VPN] > [Advanced] > [Maximum VPN Sessions] を選択します。
- ステップ 2 [最大 AnyConnect クライアントセッション数 (Maximum Sessions)] フィールドにセッションの最大許容数を入力します。

有効値は、1 からのライセンスで許容されるセッションの最大数までです。

ステップ 3 [Maximum Other VPN Sessions] フィールドで、許可する最大の VPN セッション数を入力します。これには、Cisco VPN クライアント (IPsec IKEv1) と LAN-to-LAN VPN セッションが含まれます。

有効値は、1 からのライセンスで許容されるセッションの最大数までです。

ステップ 4 [Apply] をクリックします。

DTLS の設定

Datagram Transport Layer Security (DTLS) を使用すると、SSL VPN 接続を確立している AnyConnect クライアントで、2 つのトンネル (SSL トンネルと DTLS トンネル) を同時に使用できます。DTLS を使用すると、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。

始める前に

このヘッドエンドで DTLS を設定し、使用する DTLS のバージョンを確認するには、[SSL 設定](#) を参照してください。

DTLS を TLS 接続にフォールバックさせるには、デッドピア検知 (DPD) をイネーブルにする必要があります。DPD をイネーブルにしない場合、DTLS 接続で問題が発生すると、TLS にフォールバックする代わりに接続は終了します。DPD の詳細については、[内部グループポリシー](#)、[AnyConnect クライアント](#)、[デッドピア検出 \(41 ページ\)](#) を参照してください。

手順

ステップ 1 AnyConnect クライアント VPN 接続に対して DTLS オプションを指定します。

- a) [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [Secure Client AnyConnect 接続プロファイル (AnyConnect Connection Profiles)] [アクセスインターフェイス (Access Interfaces)] セクションに移動します。
- b) [インターフェイス (Interface)] テーブルの AnyConnect クライアント 接続に設定するインターフェイスの行で、インターフェイスでイネーブルにするプロトコルをオンにします。
 - [SSL Access / Allow Access] をオンにするかイネーブルにした場合、[Enable DTLS] はデフォルトでオンまたはイネーブルになります。
 - DTLS を無効にするには、[Enable DTLS] をオフにします。SSL VPN 接続は SSL VPN トンネルのみに接続します。
- c) [Port Settings] を選択し、**SSL ポート**を設定します。

- [HTTPS Port] : HTTPS (ブラウザベース) SSL 接続用にイネーブルにするポート。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。
- [DTLS Port] : DTLS 接続用にイネーブルにする UDP ポート。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。

ステップ 2 特定のグループ ポリシーに対して DTLS オプションを指定します。

- a) [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [グループポリシー (Group Policies)] > [追加/編集 (Add/Edit)] > [詳細設定 (Advanced)] > [AnyConnect クライアント] に移動します。
- b) [Datagram Transport Layer Security (DTLS)] の [Inherit] (デフォルト)、[Enable]、または [Disable] を選択します。
- c) [DTLS Compression] の [Inherit] (デフォルト)、[Enable]、または [Disable] を選択し、DTLS の圧縮を設定します。

DNS サーバー グループの設定

[Configuration] > [Remote Access VPN] > [DNS] ダイアログボックスでは、サーバーグループ名、サーバー、タイムアウトの秒数、許容リトライ回数、およびドメイン名を含む、設定済みの DNS サーバーがテーブルに表示されます。このダイアログボックスで、DNS サーバー グループを追加、編集、または削除できます。

- [Add or Edit] : [Add or Edit DNS Server Group] ダイアログボックスが開きます。別の場所にあるヘルプ
- [Delete] : 選択した行をテーブルから削除します。確認されず、やり直しもできません。
- [DNS Server Group] : この接続の DNS サーバー グループとして使用するサーバーを選択します。デフォルトは DefaultDNS です。
- [Manage] : [Configure DNS Server Group] ダイアログボックスが開きます。

暗号化コアのプールの設定

対称型マルチプロセッシング (SMP) プラットフォームでの暗号化コアの割り当てを変更して、AnyConnect クライアント TLS/DTLS トラフィックのスループットを向上させることができます。この変更によって、SSL VPN データパスが高速化され、AnyConnect クライアント、スマートトンネル、およびポート転送において、ユーザーが認識できるパフォーマンス向上が実現します。次の手順では、シングル コンテキスト モードまたはマルチ コンテキスト モードで暗号化コアのプールを設定します。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Advanced] > [Crypto Engine] を選択します。

ステップ 2 [Accelerator Bias] ドロップダウンリストから、暗号アクセラレータプロセッサの割り当て方法を選択します。

(注) このフィールドは、機能がデバイスで使用可能な場合にだけ表示されます。

- [balanced] : 暗号化ハードウェアリソースを均等に分散します (Admin/SSL および IPsec コア)。
- [ipsec] : IPsec を優先するように暗号化ハードウェアリソースを割り当てます (SRTP 暗号化音声トラフィックを含む)。
- [ssl] : Admin/SSL を優先するように暗号化ハードウェアリソースを割り当てます。SSL ベースの AnyConnect クライアントリモートアクセス VPN セッションをサポートする場合は、このバイアスを使用します。

ステップ 3 [Apply] をクリックします。

SSL VPN 接続用のクライアントアドレス指定

このダイアログボックスを使用して、グローバルクライアントアドレスの割り当てポリシーを指定し、インターフェイスに固有のアドレスプールを設定します。このダイアログボックスを使用して、インターフェイスに固有のアドレスプールを追加、編集、または削除することもできます。ダイアログボックス下部のテーブルには、設定されているインターフェイス固有のアドレスプールの一覧が表示されます。

- [Global Client Address Assignment Policy] : すべての IPsec 接続と SSL VPN Client 接続 (AnyConnect クライアント接続を含む) に影響するポリシーを設定します。ASA は、アドレスを見つけるまで、選択されたソースを順番に使用します。
 - [Use authentication server] : クライアントアドレスのソースとして、ASA が認証サーバーの使用を試みるように指定します。
 - [Use DHCP] : クライアントアドレスのソースとして、ASA が DHCP の使用を試みるように指定します。
 - [Use address pool] : クライアントアドレスのソースとして、ASA がアドレスプールの使用を試みるように指定します。
- [Interface-Specific IPv4 Address Pools] : 設定されているインターフェイス固有のアドレスプールの一覧を表示します。
- [Interface-Specific IPv6 Address Pools] : 設定されているインターフェイス固有のアドレスプールの一覧を表示します。

- **[Add]** : **[Assign Address Pools to Interface]** ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスおよび割り当てられているアドレスプールを選択できます。
- **[Edit]** : インターフェイスとアドレスプールのフィールドに値が取り込まれた状態で、**[Assign Address Pools to Interface]** ダイアログボックスが開きます。
- **[Delete]** : 選択したインターフェイスに固有のアドレスプールを削除します。確認されず、やり直しもできません。

Assign Address Pools to Interface

このダイアログボックスを使用して、インターフェイスを選択し、そのインターフェイスにアドレスプールを1つ以上割り当てます。

- **[Interface]** : アドレスプールの割り当て先インターフェイスを選択します。デフォルトはDMZです。
- **[Address Pools]** : 指定したインターフェイスに割り当てられているアドレスプールを指定します。
- **[Select]** : **[Select Address Pools]** ダイアログボックスが開きます。このダイアログボックスでは、このインターフェイスに割り当てられているアドレスプールを1つ以上選択できます。選択内容は、**[Assign Address Pools to Interface]** ダイアログボックスの **[Address Pools]** フィールドに表示されます。

Select Address Pools

[Select Address Pools] ダイアログボックスには、クライアントアドレスの割り当てで選択可能なプール名、開始アドレスと終了アドレス、およびアドレスプールのサブネットマスクが表示され、リストのエントリを追加、編集、削除できます。

- **[Add]** : **[Add IP Pool]** ダイアログボックスが開きます。このダイアログボックスでは、新しいIPアドレスプールを設定できます。
- **[Edit]** : **[Edit IP Pool]** ダイアログボックスが開きます。このダイアログボックスでは、選択したIPアドレスプールを変更できます。
- **[Delete]** : 選択したアドレスプールを削除します。確認されず、やり直しもできません。
- **[Assign]** : インターフェイスに割り当てられているアドレスプール名を表示します。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。**[Assign]** フィールドのプール割り当て一覧が更新されます。

Add or Edit an IP Address Pool

IPアドレスプールを設定または変更します。

- **[Name]** : IPアドレスプールに割り当てられている名前を指定します。
- **[Starting IP Address]** : プールの最初のIPアドレスを指定します。
- **[Ending IP Address]** : プールの最後のIPアドレスを指定します。

- [Subnet Mask] : プール内のアドレスに適用するサブネット マスクを選択します。

グループポリシー

グループポリシーは、ASA の内部（ローカル）または外部の RADIUS または LDAP サーバーに格納されているユーザー指向の属性と値のペアのセットです。VPN 接続を確立する際に、グループポリシーによってクライアントに属性が割り当てられます。デフォルトでは、VPN ユーザーにはグループポリシーが関連付けられません。グループポリシー情報は、VPN 接続プロファイル（トンネルグループ）およびユーザーアカウントで使用されます。

ASA 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。デフォルトグループパラメータは、すべてのグループおよびユーザーに共通であると考えられるパラメータで、コンフィギュレーションタスクの効率化に役立ちます。新しいグループはこのデフォルトグループからパラメータを「継承」でき、ユーザーは自身のグループまたはデフォルトグループからパラメータを「継承」できます。これらのパラメータは、グループおよびユーザーを設定するときに上書きできます。

内部グループポリシーと外部グループポリシーを設定できます。内部グループポリシーはローカルに保存され、外部グループは RADIUS サーバーまたは LDAP サーバーに外部で保存されます。

[Group Policy] ダイアログボックスで、次の種類のパラメータを設定します。

- 一般属性 : 名前、バナー、アドレスプール、プロトコル、フィルタリング、および接続の設定。
- サーバー : DNS および WINS サーバー、DHCP スコープ、およびデフォルトドメイン名。
- 詳細属性 : スプリットトンネリング、IE ブラウザプロキシ、AnyConnect クライアント、および IPsec クライアント。

これらのパラメータを設定する前に、次の項目を設定する必要があります。

- アクセス時間 ([General] > [More Options] > [Access Hours]) 。
- フィルタ ([General] > [More Options] > [Filters]) 。
- IPsec セキュリティ アソシエーション ([Configuration] > [Policy Management] > [Traffic Management] > [Security Associations]) 。
- フィルタリングおよびスプリット トンネリング用のネットワーク リスト ([Configuration] > [Policy Management] > [Traffic Management] > [Network Lists]) 。
- ユーザー認証サーバーと内部認証サーバー ([Configuration] > [System] > [Servers] > [Authentication]) 。

次のタイプのグループポリシーを設定できます。

- [外部グループポリシー \(10 ページ\)](#) : 外部グループポリシーは、RADIUS または LDAP サーバーを ASA に示し、内部グループポリシーに設定されているようなポリシー情報の

大部分を取得できるようにします。外部グループポリシーは、ネットワーク（クライアント）アクセス VPN 接続、およびサイト間 VPN 接続に対して同じ方法で設定されます。

- [内部グループポリシー（12 ページ）](#)：これらの接続は、エンドポイントにインストールされている VPN クライアントによって開始されます。Secure Client および Cisco IPsec VPN クライアントは、VPN クライアントの使用例です。VPN クライアントが認証されると、オンサイトの場合、リモートユーザーは企業ネットワークまたはアプリケーションにアクセスできます。リモートユーザーと企業ネットワーク間のデータトラフィックは、暗号化によってインターネットを通過する際に保護されます。
- [AnyConnect クライアント内部グループポリシー（19 ページ）](#)
- [サイト間内部グループポリシー（49 ページ）](#)

[Group Policy] ペイン フィールド

ASDM の [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] ペインには、設定済みのグループポリシーが一覧表示されます。VPN グループポリシーを管理するための [Add]、[Edit]、および [Delete] ボタンを以下に示します。

- [Add]：ドロップダウンリストが表示され、内部または外部のグループポリシーを追加するかどうかを選択できます。単に [Add] をクリックする場合は、デフォルトにより内部グループポリシーを作成することになります。[Add] をクリックすると、[Add Internal Group Policy] ダイアログボックスまたは [Add External Group Policy] ダイアログボックスが開きます。これらのダイアログボックスを使用して、新しいグループポリシーを一覧に追加できます。このダイアログボックスには、3つのメニューセクションがあります。それぞれのメニュー項目をクリックすると、その項目のパラメータが表示されます。項目間を移動するとき、ASDM は設定を保持します。すべてのメニューセクションでパラメータの設定が終了したら、[Apply] または [Cancel] をクリックします。
- [Edit]：[Edit Group Policy] ダイアログボックスを表示します。このダイアログボックスを使用して、既存のグループポリシーを編集できます。
- [Delete]：AAA グループポリシーをリストから削除します。確認されず、やり直しもできません。
- [Assign]：1つ以上の接続プロファイルにグループポリシーを割り当てることができます。
- [Name]：現在設定されているグループポリシーの名前を一覧表示します。
- [Type]：現在設定されている各グループポリシーのタイプを一覧表示します。
- [Tunneling Protocol]：現在設定されている各グループポリシーが使用するトンネリングプロトコルを一覧表示します。
- [Connection Profiles/Users Assigned to]：このグループポリシーに関連付けられた ASA に直接設定された接続プロファイルとユーザーを示します。

外部グループポリシー

外部グループポリシーは、外部サーバーから認可および認証の属性値を取得します。このグループポリシーによって、ASA が属性を照会できる RADIUS または LDAP サーバーグループを特定し、それらの属性を取得するときに使用するパスワードを指定します。

ASA での外部グループ名は、RADIUS サーバーのユーザー名を参照しています。つまり、ASA に外部グループ X を設定した場合、RADIUS サーバーはクエリーをユーザー X に対する認証要求と見なします。したがって、外部グループは、ASA にとって特別な意味を持つ RADIUS サーバー上のユーザーアカウントにすぎません。外部グループ属性が認証する予定のユーザーと同じ RADIUS サーバーに存在する場合、それらの間で名前を重複させることはできません。

外部サーバーを使用するように ASA を設定する前に、適切な ASA 認可属性を指定してサーバーを設定し、それらの属性のサブセットから個々のユーザーに対する特定の許可を割り当てる必要があります。外部サーバーを設定するには、「認可および認証用の外部サーバー」の説明に従ってください。

これらの RADIUS 設定には、ローカル認証の RADIUS、Active Directory/Kerberos Windows DC の RADIUS、NT/4.0 ドメインの RADIUS、LDAP の RADIUS が含まれます。

外部グループポリシーのフィールド

- [Name] : 追加または変更するグループポリシーを特定します。[Edit External Group Policy] の場合、このフィールドは表示専用です。
- [Server Group] : このポリシーの適用先として利用できるサーバーグループを一覧表示します。
- [New] : 新しい RADIUS サーバーグループまたは新しい LDAP サーバーグループを作成するかどうかを選択できるダイアログボックスを開きます。どちらの場合も [Add AAA Server Group] ダイアログボックスが開きます。
- [Password] : このサーバーグループポリシーのパスワードを指定します。

AAA サーバーの作成および設定については、『Cisco ASA Series General Operations ASDM Configuration Guide』の「AAA Servers and Local Database」の章を参照してください。

AAA サーバーによるパスワード管理

ASA は、RADIUS および LDAP プロトコルのパスワード管理をサポートしています。

「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。その他のパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバー、LDAP サーバーなどの AAA サーバーで有効です。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。



- (注) 現在のところ MS-CHAP をサポートしていても、MS-CHAPv2 はサポートしていない RADIUS サーバーもあります。この機能には MS-CHAPv2 が必要なため、ベンダーに確認してください。

ASA では、通常、LDAP による認証時または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- Cisco Secure Client AnyConnect VPN クライアントの
- IPsec VPN クライアント
- IPsec IKEv2 クライアント

Kerberos/Active Directory (Windows パスワード) または NT 4.0 ドメインでは、パスワード管理はサポートされません。一部の RADIUS サーバー (Cisco ACS など) は、認証要求を別の認証サーバーにプロキシする場合があります。ただし、ASA からは RADIUS サーバーとだけ通信しているように見えます。



- (注) LDAP でパスワードを変更するには、市販の LDAP サーバーごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバーに対してのみ、独自のパスワード管理ロジックを実装しています。

ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

AnyConnect クライアントによるパスワードのサポート

ASA では、AnyConnect クライアントの次のパスワード管理機能をサポートします。

- ユーザーが接続しようとしたときのパスワード期限切れの通知。
- パスワードの期限が切れる前のパスワード期限切れのリマインダ。
- パスワード期限切れの無効化。ASA は AAA サーバーからのパスワード期限切れの通知を無視し、ユーザーの接続を許可します。

パスワード管理を設定すると、ASA は、リモートユーザーがログインしようとしたときに、現在のパスワードの期限が切れていること、または期限切れが近づいていることを通知します。それから ASA は、ユーザーがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザーはその古いパスワードを使用してログインし続けて、後でパスワードを変更することができます。

AnyConnect クライアントはパスワードの変更を開始できず、AAA サーバーからの変更要求に ASA を介して応答することしかできません。AAA サーバーは、AD にプロキシする RADIUS サーバー、または LDAP サーバーにする必要があります。

ASA は、次の条件下ではパスワード管理をサポートしません。

- ローカル（内部）認証を使用する場合
- LDAP 認証を使用する場合
- RADIUS 認証のみを使用しており、ユーザーが RADIUS サーバー データベースに存在する場合

パスワード期限切れの無効化を設定すると、ASA は AAA サーバーからの `account-disabled` インジケータを無視するようになります。これは、セキュリティ上のリスクになる可能性があります。たとえば、管理者のパスワードを変更しないようにする場合があります。

パスワード管理をイネーブルにすると、ASA は AAA サーバーに MS-CHAPv2 認証要求を送信します。

内部グループポリシー

内部グループポリシー、一般属性

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] ペインで、[Add or Edit Group Policy] ダイアログボックスを使用すると、追加または変更するグループポリシーのトンネリングプロトコル、フィルタ、接続設定、およびサーバーを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルトグループポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

ASDM で [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] を選択して、内部グループポリシーの一般属性を設定します。次の属性は、SSL VPN セッションと IPsec セッションに適用されます。そのため、いくつかの属性は、1 つのタイプのセッションに表示され、他のタイプには表示されません。

- [Name] : このグループポリシーの名前を最大 64 文字で指定します（スペースの使用可）。Edit 機能の場合、このフィールドは読み取り専用です。
- [Banner] : ログイン時にユーザーに対して表示するバナーテキストを指定します。長さは最大 4000 文字です。デフォルト値はありません。

IPsec VPN クライアントは、バナー用の完全な HTML をサポートしています。ただし、クライアントレスポータルおよび AnyConnect クライアントは部分的な HTML をサポートしています。バナーがリモートユーザーに適切に表示されるようにするには、次のガイドラインに従います。

- IPsec クライアント ユーザーの場合は、`\n` タグを使用します。
- AnyConnect クライアント用 ユーザーは `
` タグを使用してください。

- [SCEP forwarding URL] : CA のアドレス。クライアントプロファイルで SCEP プロキシを設定する場合に必要です。
- [Address Pools] : このグループポリシーで使用する 1 つ以上の IPv4 アドレス プールの名前を指定します。[Inherit] チェックボックスがオンの場合、グループポリシーはデフォルトグループポリシーで指定されている IPv4 アドレス プールを使用します。IPv4 アドレス プールを追加または編集する方法の詳細については、を参照してください。



(注) 内部グループポリシーで IPv4 と IPv6 両方のアドレス プールを指定できます。

[Select] —このボタンをアクティブにするには、[Inherit] チェックボックスをオフにします。[Select] をクリックして、[Address Pools] ダイアログボックスを開きます。このダイアログボックスには、クライアント アドレス割り当てで選択可能なアドレス プールのプール名、開始アドレスと終了アドレス、およびサブネットマスクが表示され、そのリストからエントリを選択、追加、編集、削除、および割り当てできます。

- [IPv6 Address Pools] : このグループポリシーで使用する 1 つ以上の IPv6 アドレス プールの名前を指定します。

[Select] —このボタンをアクティブにするには、[Inherit] チェックボックスをオフにします。[Select] をクリックすると、前述のような [Select Address Pools] ダイアログボックスが開きます。IPv6 アドレス プールを追加または編集する方法の詳細については、を参照してください。

- [More Options] : フィールドの右側にある下矢印をクリックすると、このグループポリシーのその他の設定可能なオプションが表示されます。
- [Tunneling Protocols] : このグループが使用できるトンネリングプロトコルを指定します。ユーザーは、選択されているプロトコルだけを使用できます。次の選択肢があります。
 - [Clientless SSL VPN] : SSL/TLS による VPN の使用を指定します。この VPN では、ソフトウェアやハードウェアのクライアントは必要なく、Web ブラウザを使用して ASA へのセキュアなリモートアクセス トンネルが確立されます。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有 (Web 対応)、電子メール、およびその他の TCP ベースアプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
 - [SSL VPN クライアント (SSL VPN Client)] : Cisco AnyConnect VPN Client またはレガシー SSL VPN クライアントの AnyConnect VPN モジュールの使用を指定します。AnyConnect クライアントを使用している場合は、このプロトコルを選択して Mobile User Security (MUS) がサポートされるようにする必要があります。
 - [IPsec IKEv1] : IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site (ピ

アツーパー) 接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。

- [IPsec IKEv2] : Secure Clientによってサポートされています。IKEv2 を使用した IPsec を使用するAnyConnect クライアント接続では、ソフトウェアアップデート、クライアントプロファイル、GUIのローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- [L2TP over IPsec] : 一部の一般的 PC やモバイル PC のオペレーティングシステムで提供される VPN クライアントを使用しているリモートユーザーは、L2TP over IPsec によって、パブリック IP ネットワーク経由でセキュリティアプライアンスやプライベート企業ネットワークへのセキュアな接続を確立できます。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。セキュリティアプライアンスは、IPsec 転送モード用に設定する必要があります。
- [Filter] : IPv4 または IPv6 接続で使用するアクセス コントロールリストを指定するか、グループポリシーから値を継承するかどうかを指定します。フィルタは複数のルールから構成されています。これらのルールは、ASA を介して着信したトンネリング データ パケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。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。フィルタおよびルールを設定するには、[Manage] をクリックします。
- [NAC Policy] : このグループポリシーに適用するネットワークアドミッションコントロールポリシーの名前を選択します。オプションの NAC ポリシーを各グループポリシーに割り当てることができます。デフォルト値は --None-- です。
- [Manage] : [Configure NAC Policy] ダイアログボックスが開きます。1 つ以上の NAC ポリシーを設定すると、[NAC Policy] 属性の横のドロップダウン リストに、設定した NAC ポリシー名がオプションとして表示されます。
- [Access Hours] : このユーザーに適用される既存のアクセス時間ポリシーがある場合はその名前を選択するか、または新しいアクセス時間ポリシーを作成します。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [--Unrestricted--] です。[Manage] をクリックして、[Browse Time Range] ダイアログボックスを開きます。このダイアログボックスでは、時間範囲を追加、編集、または削除できます。
- [Simultaneous Logins] : このユーザーに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザーアクセスを禁止します。



(注) 最大数の制限はありませんが、複数の同時接続の許可が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。

- **[Restrict Access to VLAN]** : (オプション) 「VLAN マッピング」とも呼ばれます。このパラメータにより、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。ASA は、このグループからのすべてのトラフィックを指定された 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。ドロップダウンリストには、デフォルト値 ([無制限 (Unrestricted)]) の他に、この ASA で設定されている VLAN だけが表示されます。



(注) この機能は、HTTP 接続の場合には有効ですが、FTP および CIFS 接続では使用できません。

- **[Connection Profile (Tunnel Group) Lock]** : このパラメータを使用すると、選択された接続プロファイル (トンネルグループ) を使用する VPN アクセスのみを許可し、別の接続ファイルを使用するアクセスを回避できます。デフォルトの継承値は [None] です。
- **Maximum Connect Time** : [Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザー接続時間を分単位で設定します。

ここで指定した時間が経過すると、システムは接続を終了します。最小値は1分、最大値は35791394分です。制限なしの接続時間を許可するには、[Unlimited] をオンにします (デフォルト)。
- **Idle Timeout** : [Inherit] チェックボックスをオフにした場合、このパラメータでアイドル時間を分単位で設定します。

この期間に接続で通信アクティビティがない場合、接続は終了します。最小時間は1分、最大時間は10080分であり、デフォルトは30分です。接続時間を無制限にするには、[Unlimited] をオンにします。
- **[Security Group Tag (SGT)]** : このグループポリシーで接続する VPN ユーザーに割り当てられる SGT タグの数値を入力します。
- **[On smart card removal]** : デフォルトのオプション [Disconnect] を選択した場合は、認証に使用されるスマートカードが取り外されると、クライアントは接続を切断します。接続の間、スマートカードをコンピュータに保持することをユーザーに要求しない場合は、[Keep the connection] をクリックします。

スマートカードの取り外しに関する設定は、RSA スマートカードを使用する Microsoft Windows でのみ機能します。
- **[同時セッションプリエンプレションで遅延のないトンネル削除を無効にする (Disable Delete tunnel with no delay in Simultaneous Session preemt)]** : 特定のユーザーが許可された [同時ログイン (Simultaneous Logins)] の制限に達すると、ユーザーの次のログイン試行では、最も古いセッションを最初に削除する必要があります。この削除には数秒かかることがあります。ユーザーが新しいセッションをすぐに確立できない場合があります。最も古いセッ

セッションの削除完了を待たずに新しいセッションを確立するようにシステムに指示するには、このオプションを選択します。

- **Maximum Connection Time Alert Interval** : ユーザーにメッセージを表示する、最大接続時間に達するまでの時間間隔。

[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、セッションアラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ~ 30 分のセッションアラート間隔を指定します。

- **Periodic Certificate Authentication Interval** : 証明書認証が定期的に再実行されるまでの時間間隔 (時間単位)。

[Inherit] チェックボックスがオフになっている場合、定期的な証明書検証の実行間隔を設定できます。範囲は 1 ~ 168 時間で、デフォルトは無効になっています。無制限の検証を許可するには、[Unlimited] をオンにします。

内部グループポリシーの設定、サーバー属性

[Group Policy] > [Servers] ウィンドウで、DNS サーバー、WINS サーバーおよび DNS スコープを設定します。DNS および WINS サーバーはフルトンネルクライアント (IPsec、AnyConnect クライアント、SVC、L2TP/IPsec) のみに適用され、名前解決に使用されます。DHCP スコープは、DHCP アドレス割り当てが設定されている場合に使用されます。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Servers] を選択します。

ステップ 2 DefaultGroupPolicy を編集する場合を除き、[DNSサーバーの継承 (DNS Servers Inherit)] チェックボックスをオフにして、このグループで使用する DNS サーバーの IPv4 または IPv6 アドレスを追加します。2つの IPv4 アドレスと 2つの IPv6 アドレスを指定できます。

複数の DNS サーバーを指定する場合、リモートアクセスクライアントは、このフィールドで指定された順序で DNS サーバーを使用しようとします。

ここで行った変更は、ASDM のこのグループポリシーを使用しているクライアントの [Configuration] > [Remote Access VPN] > [DNS] ウィンドウで設定された DNS 設定より優先されます。

ステップ 3 [WINSサーバーの継承 (WINS Servers Inherit)] チェックボックスをオフにして、プライマリおよびセカンダリ WINS サーバの IP アドレスを入力します。最初に指定する IP アドレスがプライマリ WINS サーバーの IP アドレスです。2 番目 (任意) の IP アドレスはセカンダリ WINS サーバーの IP アドレスです。

ステップ 4 [More Options] バーの二重矢印をクリックして、[More Options] エリアを展開します。

ステップ 5 [DHCPスコープの継承 (DHCP Scope Inherit)] をオフにして、DHCP スコープを定義します。

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入力します。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。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。

ステップ 6 デフォルトドメインが [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [DNS] ウィンドウで指定されていない場合は、[デフォルトドメイン (Default Domain)] フィールドでデフォルトドメインを指定する必要があります。たとえば、example.com というドメイン名とトップ レベル ドメインを使用します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

内部グループポリシー、ブラウザ プロキシ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [Browser Proxy]

このダイアログボックスでは、Microsoft Internet Explorer の設定を再構成するためにクライアントにプッシュダウンされる属性を設定します。

- [Proxy Server Policy] : クライアント PC の Microsoft Internet Explorer ブラウザのプロキシアクション (「メソッド」) を設定します。
 - [Do not modify client proxy settings] : このクライアント PC の Internet Explorer の HTTP ブラウザ プロキシ サーバー設定を変更しません。
 - [Do not use proxy] : クライアント PC の Internet Explorer の HTTP プロキシ設定をディセーブルにします。
 - [Select proxy server settings from the following] : 選択内容に応じて、[Auto detect proxy]、[Use proxy server settings given below]、および [Use proxy auto configuration (PAC) given below] のチェックボックスをオンにします。

- [Auto-detect proxy] : クライアント PC で、Internet Explorer の自動プロキシ サーバー検出の使用をイネーブルにします。
- [Use proxy server settings specified below] : [Proxy Server Name or IP Address] フィールドで設定された値を使用するように、Internet Explorer の HTTP プロキシ サーバー設定値を設定します。
- [Use proxy auto configuration (PAC) given below] : [Proxy Auto Configuration (PAC)] フィールドで指定したファイルを、自動コンフィギュレーション属性のソースとして使用するように指定します。
- [Proxy Server Settings] : Microsoft Internet Explorer を使用して、Microsoft クライアントのプロキシ サーバー パラメータを設定します。
 - [Server Address and Port] : このクライアント PC で適用される、Microsoft Internet Explorer サーバーの IP アドレスまたは名前、およびポートを指定します。
 - [Bypass Proxy Server for Local Addresses] : クライアント PC での Microsoft Internet Explorer ブラウザ プロキシ ローカルバイパス設定値を設定します。[Yes] を選択するとローカルバイパスがイネーブルになり、[No] を選択するとローカルバイパスがディセーブルになります。
 - [Exception List] : プロキシ サーバー アクセスから除外するサーバーの名前と IP アドレスを一覧表示します。プロキシサーバー経由のアクセスを行わないアドレスのリストを入力します。このリストは、[Internet Explorer の Proxy Settings] ダイアログボックスにある [Exceptions] リストに相当します。
- [Proxy Auto Configuration Settings] : PAC URL は自動設定ファイルの URL を指定します。このファイルには、ブラウザがプロキシ情報を探せる場所が記述されています。プロキシ自動コンフィギュレーション (PAC) 機能を使用する場合、リモートユーザーは、Cisco AnyConnect VPN クライアントを使用する必要があります。

多くのネットワーク環境が、Web ブラウザを特定のネットワーク リソースに接続する HTTP プロキシを定義しています。HTTP トラフィックがネットワーク リソースに到達できるのは、プロキシがブラウザに指定され、クライアントが HTTP トラフィックをプロキシにルーティングする場合だけです。SSLVPN トンネルにより、HTTP プロキシの定義が複雑になります。企業ネットワークにトンネリングするときに必要なプロキシが、ブロードバンド接続経由でインターネットに接続されるときや、サードパーティ ネットワーク上にあるときに必要なものとは異なることがあるためです。

また、大規模ネットワークを構築している企業では、複数のプロキシサーバーを設定し、一時的な状態に基づいてユーザーがその中からプロキシサーバーを選択できるようにすることが必要になる場合があります。pac ファイルを使用すると、管理者は数多くのプロキシからどのプロキシを社内のすべてのクライアントコンピュータに使用するかを決定する単一のスクリプト ファイルを作成できます。

次に、PAC ファイルを使用する例をいくつか示します。

- ロード バランシングのためリストからプロキシをランダムに選択します。

- サーバーのメンテナンススケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
- プライマリ プロキシで障害が発生した場合に備えて、使用するバックアッププロキシサーバーを指定します。
- ローカルサブネットを元に、ローミングユーザー用に最も近いプロキシを指定します。

テキストエディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション (.pac) ファイルを作成できます。 .pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシサーバーを指定するロジックを含む JavaScript ファイルです。 [PAC URL] フィールドを使用して、 .pac ファイルの取得元 URL を指定します。 ブラウザは、 .pac ファイルを使用してプロキシ設定を判断します。

• Proxy Lockdown

- [クライアントシステムのプロキシロックダウンを許可 (Allow Proxy Lockdown for Client System)] : この機能をイネーブルにすると、 AnyConnect クライアント VPN セッションの間、 Microsoft Internet Explorer の [接続 (Connections)] タブが非表示になります。 また、 Windows 10 バージョン 1703 (以降) では、この機能を有効にすると、 AnyConnect クライアント VPN セッションの間、設定アプリのシステムプロキシタブも非表示になります。 この機能を無効にしても、 Microsoft Internet Explorer の [Connections] タブと設定アプリのプロキシタブの表示は変わりません。 これらのタブのデフォルト設定は、ユーザーのレジストリ設定に応じて表示または非表示になります。



(注) AnyConnect VPN セッションの間、設定アプリのシステムプロキシタブを非表示にするには、AnyConnect クライアントバージョン 4.7.03052 以降が必要です。

AnyConnect クライアント内部グループポリシー

内部グループポリシー、詳細、AnyConnect クライアント

- [Keep Installer on Client System] : リモート コンピュータ上で永続的なクライアントのインストールを可能にします。これをイネーブルにすることにより、クライアントの自動的なアンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモート コンピュータにインストールされたままなので、リモートユーザーの接続時間が短縮されます。
- [Compression] : 圧縮を行うと、転送されるパケットのサイズが減少するため、セキュリティアプライアンスとクライアント間の通信パフォーマンスが向上します。

- [Datagram TLS] : Datagram Transport Layer Security により、一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、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を改善します。
- [Ignore Don't Defrag (DF) Bit] : この機能では、DF ビットが設定されているパケットを強制的にフラグメンテーションして、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバーに対する使用などがあります。
- [クライアントバイパスプロトコル (Client Bypass Protocol)] : クライアントプロトコルバイパス機能を使用すると、ASA が IPv6 トラフィックだけを予期しているときの AnyConnect クライアントクライアントによる IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定することができます。

AnyConnect クライアントが ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ASA が AnyConnect クライアント接続に IPv4 アドレスまたは IPv6 アドレスだけを割り当てた場合に、ASA 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、または ASA 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を設定できるようになりました。

たとえば、ASA が AnyConnect クライアント接続に IPv4 アドレスのみを割り当て、エンドポイントがデュアルスタックされているとします。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機能がディセーブルの場合は、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イネーブルの場合は、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。

SSL 接続ではなく IPsec トンネルを確立している場合は、クライアントで IPv6 が有効になっているかどうか ASA に通知されないため、ASA は常にクライアントバイパスプロトコル設定をプッシュダウンします。

- [FQDN of This Device] : この情報は、VPN セッションの再確立で使用される ASA IP アドレスを解決するために、ネットワークローミングの後でクライアントに使用されます。この設定は、さまざまな IP プロトコルのネットワーク間のローミングをサポートするうえで重要です (IPv4 から IPv6 など) 。



- (注) AnyConnect クライアント プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロードバランシングシナリオの正しいデバイス (トンネルが確立されているデバイス) と一致しない場合があります。

デバイスの FQDN がクライアントに配信されない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル (IPv4 から IPv6) のネットワーク間のローミングをサポートするには、AnyConnect クライアントは、トンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDN の名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、使用可能な場合は常に、ASA によってプッシュされた (また、グループ ポリシーで管理者が設定した) デバイス FQDN を使用します。FQDN が設定されていない場合、ASA は、[Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得 (およびクライアントに送信) します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

- [MTU] : SSL 接続の MTU サイズを調整します。256 ~ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLS のオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。
- [Keepalive Messages] : [Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブメッセージの間隔をイネーブルおよび調整して、プロキシ、ファイアウォール、または NAT デバイスを通じた接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモートユーザーが、Microsoft Outlook や Microsoft Internet Explorer などのソケットベースのアプリケーションを実際に行っていないときでも、クライアントが切断と再接続を行わないことが保証されます。
- [ダウンロードするオプションのクライアントモジュール (Optional Client Modules to Download)] : ダウンロード時間を短縮するために、AnyConnect クライアントは、サポートしている各機能に必要なモジュールだけを (ASA から) ダウンロードするように要求します。次のような他の機能をイネーブルにするモジュールの名前を指定する必要があります。AnyConnect クライアントには、次のモジュールが含まれています (一部の旧バージョンではモジュールの数が少なくなります)。
 - [AnyConnect クライアント DART] : Diagnostic AnyConnect クライアント Reporting Tool (DART) は、トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システムログのスナップショットおよびその他の診断情報をキャプチャし、.zip ファイルをデスクトップに作成します。
 - AnyConnect クライアント ネットワーク アクセス マネージャ : 以前は Cisco Secure Services Client と呼ばれていました。このモジュールは、有線とワイヤレスの両方のネットワークにアクセスするための 802.1X (レイヤ 2) とデバイス認証を備えています。
 - AnyConnect クライアント SBL : Start Before Logon (SBL) は、Windows のログインダイアログボックスが表示される前に AnyConnect クライアントを開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。

- **Secure Firewall** ポスチャモジュール：以前は Cisco Secure Desktop HostScan 機能と呼ばれていました。このポスチャモジュールは AnyConnect クライアントに統合され、これにより AnyConnect クライアントは、ASA へのリモートアクセス接続を確立する前にポスチャアセスメントのクレデンシャルを収集できるようになります。
- **ISE ポスチャ**：OPSWAT v3 ライブラリを使用してポスチャ チェックを実行し、エンドポイントの適合性を評価します。その後、エンドポイントが適合するまでネットワーク アクセスを制限したり、ローカル ユーザーの権限を強化したりできます。
- **AMP イネーブラ**：エンドポイント向けの高度なマルウェア防御（AMP）を導入する手段として使用されます。社内でローカルにホストされているサーバーからエンドポイントのサブセットに AMP for Endpoints ソフトウェアをプッシュし、既存のユーザーベースに AMP サービスをインストールします。
- **ネットワーク可視性モジュール**：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。NVM（ネットワーク可視性モジュール）は、エンドポイントのテレメトリを収集して、フローデータとファイルレピュテーションを syslog に記録し、さらに、ファイルの分析と UI インターフェイスの提供を行うコレクタ（サードパーティベンダー）にもフロー レコードをエクスポートします。
- **Umbrella Roaming Security** モジュール：アクティブな VPN がないときに DNS レイヤセキュリティを提供します。Cisco Umbrella Roaming と OpenDNS Umbrella サービスのいずれかに対するサブスクリプションを提供し、Intelligent Proxy および IP レイヤ適用機能を追加します。Umbrella Security Roaming プロファイルは、対応するサービスと各展開を関連付けて、対応する保護レベルを自動的に有効にします（コンテンツフィルタリング、複数のポリシー、強力なレポート、Active Directory 統合、または基本的な DNS レイヤセキュリティ）。
- **Always-On VPN**：AnyConnect クライアント サービスプロファイルの常時接続 VPN フラグ設定をディセーブルにするか、または AnyConnect クライアント サービスプロファイル設定を使用する必要があるかを決定します。常時接続 VPN 機能により、ユーザーがコンピュータにログオンすると、AnyConnect は VPN セッションを自動的に確立します。VPN セッションは、ユーザーがコンピュータからログオフするまで維持されます。物理的な接続が失われてもセッションは維持され、AnyConnect クライアントは、適応型セキュリティアプライアンスとの物理的な接続の再確立を絶えず試行し、VPN セッションを再開します。

常時接続 VPN によって、企業ポリシーを適用して、セキュリティ脅威からデバイスを保護できます。常時接続 VPN を使用して、エンドポイントが信頼ネットワーク内ではない場合にいつでも AnyConnect クライアントが VPN セッションを確立したことを確認できます。イネーブルにすると、接続が存在しない場合のネットワーク接続の管理方法を決定するポリシーが設定されます。



(注) また、常時接続 VPN にはセキュリティクライアント機能をサポートする AnyConnect クライアント リリースが必要です。

- [ダウンロードするクライアントプロファイル (Client Profiles to Download)] : プロファイルはコンフィギュレーションパラメータのグループであり、AnyConnect クライアントで VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ISE ポスチャ、AMP イネーブラ、ネットワーク可視性モジュール、および Umbrella Roaming Security モジュールの設定に使用されます。[追加 (Add)] をクリックして [AnyConnect クライアントプロファイルの選択 (Select AnyConnect Client Profiles)] ウィンドウを起動すると、以前グループポリシー用に作成されたプロファイルを指定できます。

AnyConnect クライアントトラフィックに対するスプリットトンネリングの設定

スプリットトンネリングは、一部の AnyConnect クライアント ネットワークトラフィックを VPN トンネルに誘導して通過させ (暗号化)、他のネットワークトラフィックを VPN トンネルの外に誘導します (非暗号化、つまり「クリアテキストの状態」)。

スプリット トンネリングを設定するには、スプリット トンネリング ポリシーを作成し、そのポリシーにアクセス コントロール リストを設定し、グループ ポリシーにスプリット トンネル ポリシーを追加します。グループ ポリシーをクライアントに送信する際に、クライアントはスプリット トンネリング ポリシーの ACL を使用してどこにネットワークトラフィックを送信するかを決定します。



- (注) スプリットトンネリングはセキュリティ機能ではなく、トラフィック管理機能です。最大限のセキュリティを確保するには、スプリットトンネリングをイネーブルにしないことを推奨します。

Windows クライアントでは、最初に ASA からのファイアウォールルールが評価され、次にクライアントのファイアウォールルールが評価されます。Mac OS X では、クライアントのファイアウォールルールおよびフィルタールールは使用されません。Linux システムの AnyConnect バージョン 3.1.05149 以降では、`circumvent-host-filtering` という名前のカスタム属性をグループプロファイルに追加して `true` に設定することで、クライアントのファイアウォールルールおよびフィルタールールを評価するように AnyConnect クライアント を設定できます。

アクセス リストを作成する場合：

- アクセス コントロール リストには IPv4 および IPv6 両方のアドレスを指定できます。
- 標準 ACL を使用すると、1 つのアドレスまたはネットワークのみが使用されます。
- 拡張 ACL を使用すると、ソース ネットワークがスプリット トンネリング ネットワークになります。この場合、宛先ネットワークは無視されます。
- any が設定されたアクセス リストや、`split include` または `split exclude` が `0.0.0.0/0.0.0.0` または `::/0` に設定されたアクセス リストは、クライアントに送信されません。すべてのトラフィックをトンネル経由で送信するには、スプリット トンネルの **Policy** に対して **Tunnel All Networks** を選択します。

- アドレス 0.0.0.0/255.255.255.255 または ::/128 は、スプリットトンネルポリシーが **Exclude Network List Below** の場合にのみクライアントに送信されます。この設定は、トンネルトラフィックがローカルサブネット宛でないことをクライアントに通知します。
- AnyConnect クライアントでは、スプリットトンネリングポリシーで指定されたすべてのサイト、および ASA によって割り当てられた IP アドレスと同じサブネット内にあるすべてのサイトにトラフィックが渡されます。たとえば、ASA によって割り当てられた IP アドレスが 10.1.1.1、マスクが 255.0.0.0 の場合、エンドポイントデバイスは、スプリットトンネリングポリシーに関係なく、10.0.0.0/8 を宛先とするすべてのトラフィックを渡します。そのため、割り当てられた IP アドレスが、期待されるローカルサブネットを適切に参照するように、ネットマスクを使用します。

始める前に

- 適切な ACE でアクセスリストを作成する必要があります。
- スプリットトンネルポリシーを IPv4 ネットワーク用と IPv6 ネットワーク用に作成した場合は、指定したネットワークリストが両方のプロトコルで使用されます。このため、ネットワークリストには、IPv4 および IPv6 の両方のトラフィックのアクセスコントロールエントリ (ACE) が含まれている必要があります。これらの ACL を作成していない場合は、一般的操作用コンフィギュレーションガイドを参照してください。

次の手順では、フィールドの隣に [Inherit] チェックボックスがあるすべてのケースで、[Inherit] チェックボックスがオンのままの場合、設定しているグループポリシーは、そのフィールドについて、デフォルトグループポリシーと同じ値を使用することを意味します。[Inherit] チェックボックスをオフにすると、グループポリシーに固有の新しい値を指定できます。

手順

- ステップ 1** ASDM を使用して ASA に接続し、[**Configuration**] > [**Remote Access VPN**] > [**Network (Client) Access**] > [**Group Policies**] に移動します。
- ステップ 2** [Add] をクリックして新しいグループポリシーを追加するか、既存のグループポリシーを選択して [Edit] をクリックします。
- ステップ 3** [**Advanced**] > [**Split Tunneling**] を選択します。
- ステップ 4** [DNS名 (DNS Names)] フィールドに、トンネルを介して AnyConnect クライアントで解決するドメイン名を入力します。これらの名前は、プライベートネットワーク上のホストに対応します。split-include トンネリングが設定されている場合は、指定された DNS サーバーがネットワークリストに含まれている必要があります。フィールドには、完全修飾ドメイン名、IPv4 アドレス、または IPv6 アドレスを入力できます。

ダイナミック スプリット トンネリング ドメイン名には、トップレベルドメインの他に少なくとも 1 つのドメイン名ラベルが必要です。ダイナミック スプリット トンネリングは、特定のドメイン名に一致するフローをターゲットとするようになっていたため、トップレベルドメイン (*org* など) だけを指定することはできないのです。トップレベルドメインと少なくとも 1 つのドメイン名ラベル (*domain.org* など) を入力する必要があります。

ステップ 5 スプリットトンネリングをディセーブルにするには、[Yes] をクリックして [Send All DNS Lookups Through Tunnel] をイネーブルにします。このオプションを設定すると、DNS トラフィックが物理アダプタに漏れず、クリアテキストで送信されるトラフィックが拒否されます。DNS 解決に失敗すると、アドレスは未解決のまま残ります。AnyConnect クライアントは、VPN 外のアドレスを解決しようとはしません。

スプリットトンネリングをイネーブルにするには、[No] を選択します（デフォルト）。この設定では、クライアントはスプリットトンネルポリシーに従ってトンネルを介して DNS クエリを送信します

ステップ 6 スプリットトンネリングを設定するには、[Inherit] チェックボックスをオフにして、スプリットトンネリングポリシーを選択します。[Inherit] チェックボックスをオフにしない場合、グループポリシーでは、デフォルトのグループポリシー **DfltGrpPolicy** で定義されたスプリットトンネリング設定が使用されます。デフォルトグループポリシーのスプリットトンネリングポリシーのデフォルト設定は [Tunnel All Networks] です。

スプリットトンネリングポリシーを定義するには、ドロップダウン [Policy] および [IPv6 Policy] から選択します。[Policy] フィールドでは、IPv4 ネットワークトラフィックのスプリットトンネリングポリシーを定義します。[IPv6 Policy] フィールドでは、IPv6 ネットワークトラフィックのスプリットトンネリングポリシーを選択します。そうした違い以外は、これらのフィールドの目的は同じです。

[Inherit] チェックボックスをオフにした場合は、次のいずれかのポリシーオプションを選択できます。

- [Exclude Network List Below] : クリアテキストで送信されるトラフィックの宛先ネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカルネットワーク上のデバイス（プリンタなど）にアクセスするリモートユーザーにとって役立ちます。
- [Tunnel Network List Below] : [Network List] で指定されたネットワーク間のすべてのトラフィックがトンネリングされます。インクルードネットワークリスト内のアドレスへのトラフィックがトンネリングされます。その他すべてのアドレスに対するデータは、クリアテキストで送信され、リモートユーザーのインターネットサービスプロバイダーによってルーティングされます。

ASA 9.1.4 以降のバージョンでは、インクルードリストを指定するときに、インクルード範囲内のサブネットにエクスクルードリストも指定できます。これらの除外されたサブネットはトンネリングされず、インクルードリストの残りのネットワークはトンネリングされます。インクルードリストのサブネットではないエクスクルージョンリスト内のネットワークは、クライアントで無視されます。Linux の場合、サブネットの除外をサポートするには、グループポリシーにカスタム属性を追加する必要があります。

次に例を示します。

#	Enabled	Source	User	Security Group	Destination	Security Group	Service	Action
1	<input checked="" type="checkbox"/>	10.10.10.0/24			any		IP ip	Deny
2	<input checked="" type="checkbox"/>	10.0.0.0/8			any		IP ip	Permit

(注) Split-Include ネットワークがローカルサブネットの完全一致 (192.168.1.0/24 など) の場合、対応するトラフィックはトンネリングされています。Split-Include ネットワークがローカルサブネットのスーパーセット (192.168.0.0/16 など) の場合、対応するトラフィックは、ローカルサブネットを除き、トンネリングされています。ローカルサブネットトラフィックもトンネリングするには、一致する Split-Include ネットワーク (192.168.1.0/24 および 192.168.0.0/16 の両方を Split-Include ネットワークとして指定) を追加する必要があります。

Split-Include ネットワークが無効 (0.0.0.0/0.0.0.0 など) の場合、スプリットトンネリングはディセーブルになります (すべてのトラフィックがトンネリングされます)。

- [Tunnel All Networks] : このポリシーは、すべてのトラフィックがトンネリングされるように指定します。この指定では、実質的にスプリットトンネリングは無効になります。リモートユーザーは企業ネットワークを経由してインターネットにアクセスしますが、ローカルネットワークにはアクセスできません。これがデフォルトのオプションです。

ステップ 7 [Network List] フィールドで、スプリットトンネリングポリシーを適用するアクセスコントロールリストを選択します。[Inherit] チェックボックスがオンの場合、グループポリシーはデフォルトグループポリシーで指定されているネットワークリストを使用します。

[Manage] コマンドボタンを選択して [ACL Manager] ダイアログボックスを開きます。このボックスでは、ネットワークリストとして使用するアクセスコントロールリストを設定できます。ネットワークリストを作成または編集する方法の詳細については、一般的操作コンフィギュレーションガイドを参照してください。

拡張 ACL リストには IPv4 アドレスと IPv6 アドレスの両方を含めることができます。

ステップ 8 [Intercept DHCP Configuration Message from Microsoft Clients] は DHCP 代行受信に固有の追加パラメータを示します。DHCP 代行受信によって、Microsoft XP クライアントは ASA でスプリットトンネリングを使用できるようになります。

- [Intercept] : DHCP 代行受信を許可するかどうかを指定します。[Inherit] を選択しない場合、デフォルト設定は [No] です。
- [Subnet Mask] : 使用するサブネットマスクを選択します。

ステップ 9 [OK] をクリックします。

ダイナミック スプリット トンネリングの設定

ダイナミック スプリット トンネリングでは、トンネルの確立後に、DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。ダイナミック スプリット トンネリングを設定するには、カスタム属性を作成し、グループ ポリシーに追加します。

始める前に

この機能を使用するには、AnyConnect リリース 4.5（またはそれ以降）が必要です。詳細については、「[About Dynamic Split Tunneling](#)」を参照してください。

手順

- ステップ 1** [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [アドバンス (Advanced)] > [AnyConnect クライアントカスタム属性 (Custom Attributes)] 画面を参照します。
- ステップ 2** [Add] をクリックし、dynamic-split-exclude-domains を属性タイプとして入力し、説明を入力します。
- ステップ 3** この新しい属性をクリックして適用したら、UI 画面上部にある [AnyConnect クライアント custom attribute names] リンクをクリックします。
- ステップ 4** VPN トンネル外部からのクライアントによるアクセスが必要な各クラウド/Web サービスについて、対応するカスタム属性名を追加します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。これらのドメインは、[AnyConnect クライアントカスタム属性名 (Custom Attribute Names)] 画面の [値 (Value)] 部分で、ドメインをコンマ文字で区切るコンマ区切り値 (CSV) 形式を使用して定義します。AnyConnect クライアントでは、区切り文字 (約 300 の通常サイズのドメイン名) を除く最初の 20,000 文字のみが考慮されます。その制限を超えるドメイン名は無視されます。

カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。
- ステップ 5** [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を参照し、ダイナミック スプリット除外トンネリング属性を特定のグループ ポリシーに付加します。
- ステップ 6** 新しいグループ ポリシーを作成するか、[Edit] をクリックして既存のグループ ポリシーを管理することができます。

次のタスク

スプリットを含むトンネリングが設定されている場合、ダイナミック スプリット除外は、スプリットを含むネットワークに DNS 応答 IP アドレスが 1 つ以上含まれる場合のみ、実行されません。DNS 応答 IP アドレスとスプリットを含むネットワークのいずれかの間にまったく重なりがない場合、すべての DNS 応答 IP アドレスに一致するトラフィックはすでにトンネリングから除外されているため、ダイナミック スプリット除外の実行は不要です。

ダイナミック スプリット除外トンネリングの設定

ASDM を使用してダイナミック スプリット除外トンネリングを有効にするには、次の設定手順を実行します。ダイナミック スプリット除外ドメインとインクルードドメインの両方が定義されている場合は、ドメイン名の一致による拡張ダイナミック スプリット除外トンネリングが有効になります。たとえば、管理者は `example.com` へのトラフィックを `www.example.com` 以外はすべて除外するように設定できます。`Example.com` はダイナミック スプリット除外ドメインであり、`www.example.com` はダイナミック スプリット インクルードドメインです。



- (注) ダイナミック スプリット除外トンネリングを使用するには、AnyConnect リリース 4.5 (以降) が必要です。また、AnyConnect リリース 4.6 (以降) で、両方のドメインが設定されている場合の拡張ダイナミック スプリット インクルードとスプリット除外のための改善が加えられました。ダイナミック スプリット除外は tunnel-all 設定、split-exclude 設定、および split-include 設定に適用されます。

始める前に

AnyConnect クライアントの要件については、「ダイナミック スプリット トンネリング」の項を参照してください。

手順

- ステップ 1** [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [アドバンス (Advanced)] > [AnyConnect クライアントカスタム属性 (Custom Attributes)] 画面を参照します。
- ステップ 2** [Add] をクリックし、dynamic-split-exclude-domains を属性タイプとして入力し、説明を入力します。
- ステップ 3** この新しい属性をクリックして適用したら、UI 画面上部にある [AnyConnect クライアント custom attribute names] リンクをクリックします。
- ステップ 4** VPN トンネル外部からのクライアントによるアクセスが必要な各クラウド/Web サービスについて、対応するカスタム属性名を追加します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。これらのドメインは、[AnyConnect クライアントカスタム属性名 (Custom Attribute Names)] 画面の [値 (Value)] 部分で、ドメインをコンマ文字で区切るコンマ区切り値 (CSV) 形式を使用して定義します。AnyConnect クライアントでは、区切り文字 (約 300 の通常サイズのドメイン名) を除く最初の 5000 文字のみが考慮されます。その制限を超えるドメイン名は無視されます。

カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。
- ステップ 5** [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を参照し、ダイナミック スプリット除外トンネリング属性を特定のグループポリシーに付加します。

- ステップ 6** 新しいグループポリシーを作成するか、[Edit]をクリックして既存のグループポリシーを管理することができます。
- ステップ 7** 左側のメニューで、[詳細設定 (Advanced)]>[AnyConnect クライアント]>[カスタム属性 (Custom Attributes)]をクリックし、ドロップダウンから属性タイプを選択します。

ダイナミック スプリット包含トンネリングの設定

ASDM を使用してダイナミック スプリット インクルード トンネリングを有効にするには、次の設定手順を実行します。ダイナミック スプリット除外ドメインとインクルードドメインの両方が定義されている場合は、ドメイン名の一致による拡張ダイナミック スプリット インクルード トンネリングが有効になります。たとえば、管理者は domain.com へのトラフィックを www.domain.com 以外はすべて含まれるように設定できます。Domain.com はダイナミック スプリット インクルードドメインであり、www.domain.com はダイナミック スプリット除外ドメインです。



- (注) AnyConnect リリース 4.6 (以降) があり、ダイナミック スプリット インクルード トンネリングを使用する必要があります。また、AnyConnect リリース 4.6 (以降) で、両方のドメインが設定されている場合の拡張ダイナミック スプリット インクルードとスプリット除外のための改善が加えられました。ダイナミック スプリット インクルードは split-include 設定にのみ適用されます。

始める前に

AnyConnect クライアントの要件については、「ダイナミック スプリット トンネリング」の項を参照してください。

手順

- ステップ 1** [設定 (Configuration)]>[リモートアクセスVPN (Remote Access VPN)]>[ネットワーク (クライアント) アクセス (Network (Client) Access)]>[アドバンス (Advanced)]>[AnyConnect クライアントカスタム属性 (Custom Attributes)]画面を参照します。
- ステップ 2** [Add]をクリックし、属性タイプとして dynamic-split-include-domains と入力し、説明を入力します。
- ステップ 3** この新しい属性をクリックして適用したら、UI 画面上部にある [AnyConnect クライアント custom attribute names] リンクをクリックします。
- ステップ 4** VPN トンネル外部からのクライアントによるアクセスが必要な各クラウド/Web サービスについて、対応するカスタム属性名を追加します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。これらのドメインは、[AnyConnect クライアントカスタム属性名 (Custom Attribute Names)]画面の [値 (Value)] 部分で、ドメインをコンマ文字で区切るコンマ区切り値 (CSV) 形式を使用して定義します。AnyConnect クラ

クライアントでは、区切り文字（約 300 の通常サイズのドメイン名）を除く最初の 5000 文字のみが考慮されます。その制限を超えるドメイン名は無視されます。

カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。

- ステップ 5** [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を参照して、ダイナミック スプリット インクルード トンネリング 属性を特定のグループ ポリシーに追加します。
- ステップ 6** 新しいグループ ポリシーを作成するか、[Edit] をクリックして既存のグループ ポリシーを管理することができます。
- ステップ 7** 左側のメニューで、[詳細設定 (Advanced)] > [AnyConnect クライアント] > [カスタム属性 (Custom Attributes)] をクリックし、ドロップダウンから属性タイプを選択します。

管理 VPN トンネルの設定

管理 VPN トンネルにより、エンドユーザによって VPN 接続が確立されるだけでなく、クライアント システムの電源が入るたびに社内ネットワークの接続が確保されます。オフィス ネットワークに VPN を介してユーザが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで Patch Management を行うことができます。この機能には、社内ネットワークの接続を必要とするエンドポイント OS ログインスクリプトに対するメリットもあります。

管理 VPN トンネルはエンドユーザに対し透過的であるため、ユーザアプリケーションによって開始されたネットワーク トラフィックはデフォルトで影響を受けませんが、代わりに管理 VPN トンネルの外部に転送されます。

ログインが低速であるとユーザから報告された場合、管理トンネルが適切に設定されていない可能性があります。追加の要件、非互換性、制限、および管理 VPN トンネルのトラブルシューティングについては、『Cisco Secure Client Administration Guide』を参照してください。

始める前に

AnyConnect リリース 4.7（またはそれ以降）が必要

手順

- ステップ 1** トンネルグループの認証方法は、[設定 (Configuration)] > [リモートアクセス (Remote Access)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > AnyConnect クライアント [接続プロファイル (Connection Profiles)] > [追加/編集 (Add/Edit)] に移動し、[証明書のみ (certificate only)] として設定する必要があります。
- ステップ 2** 次に、同じウィンドウで、[Advanced] > [Group Alias/Group URL] を選択し、管理 VPN プロファイルで指定するグループ URL を追加します。

- ステップ 3** このトンネル グループのグループ ポリシーには、トンネル グループで設定されたアドレス プールを使用するすべての IP プロトコルに対してスクリプト包含トンネリングが設定されている必要があります。[Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Edit] > [Advanced] > [Split Tunneling] から [Tunnel Network List Below] を選択します。
- ステップ 4** (オプション) ユーザーが開始したネットワーク通信に影響しないように (管理 VPN トンネルは透過的であるため) スプリット包含トンネリングの設定がデフォルトで必要です。この動作をオーバーライドするには、管理トンネル接続で使用されているグループポリシーにカスタム属性を設定します: [AnyConnect クライアント カスタム属性 \(118 ページ\)](#)。両方の IP プロトコルに対するトンネルグループでアドレス プールが設定されていない場合、グループ ポリシーで [Client Bypass Protocol] をイネーブルにし、アドレス プールのない IP プロトコルと一致するトラフィックが管理 VPN トンネルで中断されないようにする必要があります。
- ステップ 5** プロファイルを作成し、プロファイルの使用の管理 VPN トンネルを選択します: [AnyConnect クライアント プロファイルの設定 \(100 ページ\)](#)。

サブネットの除外をサポートするための Linux の設定

スプリットトンネリング用に [Tunnel Network List Below] を設定した場合、Linux ではサブネットの除外をサポートするために追加の設定が必要になります。circumvent-host-filtering という名前のカスタム属性を作成して true に設定し、スプリットトンネリング用に設定されたグループポリシーに関連付ける必要があります。

手順

- ステップ 1** ASDM に接続し、[設定 (Configuration)] > [リモートアクセス VPN] > [Network (Client) Access] > [詳細設定 (Advanced)] > [AnyConnect クライアントカスタム属性 (Custom Attributes)] に移動します。
- ステップ 2** [Add] をクリックし、circumvent-host-filtering という名前のカスタム属性を作成して、その値を true に設定します。
- ステップ 3** クライアントファイアウォールに対して使用予定のグループポリシーを編集し、[詳細設定 (Advanced)] > [AnyConnect クライアント] > > [カスタム属性 (Custom Attributes)] に移動します。
- ステップ 4** 作成したカスタム属性 circumvent-host-filtering をスプリット トンネリングに使用するグループポリシーに追加します。

内部グループポリシー、AnyConnect クライアント属性

[設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [グループポリシー (Group Policies)] > [追加/編集 (Add/Edit)] > [詳細設定 (Advanced)] > [AnyConnect クライアント] には、このグループポリシーで設定可能なAnyConnect クライアントの属性が表示されます。

- [Keep Installer on Client System] : リモート コンピュータ上で永続的なクライアントのインストールを可能にします。これをイネーブルにすることにより、クライアントの自動的なアンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモート コンピュータにインストールされたままなので、リモート ユーザーの接続時間が短縮されます。



(注) [インストーラーをクライアントシステムに保持 (Keep Installer on Client System)] は、AnyConnect クライアントのバージョン 2.5 以降でサポートされていません。

- [Datagram Transport Layer Security (DTLS)] : 一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、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を改善します。
- [DTLS Compression] : DTLS における圧縮を設定します。
- [SSL Compression] : SSL/TLS における圧縮を設定します。
- [Ignore Don't Defrag (DF) Bit] : この機能では、DF ビットが設定されているパケットを強制的にフラグメンテーションして、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバーに対する使用などがあります。
- [クライアントバイパスプロトコル (Client Bypass Protocol)] : クライアントプロトコルバイパスでは、ASA が IPv6 トラフィックだけを予期しているときの AnyConnect クライアントクライアントによる 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します。

AnyConnect クライアントが ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。クライアントバイパスプロトコルでは、ASA が IP アドレスを割り当てなかったトラフィックをドロップするか、または ASA 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を決定します。

たとえば、ASA が AnyConnect クライアント 接続に IPv4 アドレスのみを割り当て、エンドポイントがデュアルスタックされているとします。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機能がディセーブルの場合は、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イネーブルの場合は、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。

- [FQDN of This Device] : この情報は、VPN セッションの再確立で使用される ASA IP アドレスを解決するために、ネットワークローミングの後でクライアントに使用されます。この設定は、さまざまな IP プロトコルのネットワーク間のローミングをサポートするうえで重要です (IPv4 から IPv6 など)。



- (注) AnyConnect クライアント プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロード バランシング シナリオの正しいデバイス (トンネルが確立されているデバイス) と一致しない場合があります。

デバイスの FQDN がクライアントに配信されない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル (IPv4 から IPv6) のネットワーク間のローミングをサポートするには、AnyConnect クライアントは、トンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDN の名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、使用可能な場合は常に、ASA によってプッシュされた (また、グループ ポリシーで管理者が設定した) デバイス FQDN を使用します。FQDN が設定されていない場合、ASA は、[Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得 (およびクライアントに送信) します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

- [MTU] : SSL 接続の MTU サイズを調整します。256 ~ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLS のオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。
- [Keepalive Messages] : [Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブメッセージの間隔をイネーブルおよび調整して、プロキシ、ファイアウォール、または NAT デバイスを通じた接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモートユーザーが、Microsoft Outlook や Microsoft Internet Explorer などのソケットベースのアプリケーションを実際に行っていないときでも、クライアントが切断と再接続を行わないことが保証されます。
- [ダウンロードするオプションのクライアントモジュール (Optional Client Modules to Download)] : ダウンロード時間を短縮するために、AnyConnect クライアントは、サポートしている各機能に必要なモジュールだけを (ASA から) ダウンロードするように要求します。次のような他の機能をイネーブルにするモジュールの名前を指定する必要があります。AnyConnect クライアントのバージョン 4.0 には、次のモジュールが含まれています (旧バージョンではモジュールの数が少なくなります) 。
 - [AnyConnect クライアント DART] : Diagnostic AnyConnect クライアント Reporting Tool (DART) は、トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システムログのスナップショットおよびその他の診断情報をキャプチャし、.zip ファイルをデスクトップに作成します。
 - AnyConnect クライアント ネットワーク アクセス マネージャ : 以前は Cisco Secure Services Client と呼ばれていました。このモジュールは、有線とワイヤレスの両方の

ネットワークにアクセスするための 802.1X（レイヤ 2）とデバイス認証を備えています。

- AnyConnect クライアント SBL : Start Before Logon (SBL) は、Windows のログインダイアログボックスが表示される前に AnyConnect クライアントを開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。
- AnyConnect クライアント Web セキュリティモジュール：以前は ScanSafe Hostscan と呼ばれていました。このモジュールは、AnyConnect クライアントに統合されています。また、Web ページの要素を分解して、同時に各要素を分析できるようにします。その後、定義されているセキュリティポリシーに基づいて、受け入れ可能なコンテンツを許可し、悪意があるコンテンツや許容できないコンテンツをドロップします。
- AnyConnect クライアント テレメトリモジュール：悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティアプライアンス (WSA) に送信します。WSA では、このデータを使用して、URL のフィルタリングルールを改善します。



(注) テレメトリは AnyConnect 4.0 ではサポートされません。

- ASA ポスチャモジュール：以前は Cisco Secure Desktop HostScan 機能と呼ばれていました。このポスチャモジュールは AnyConnect クライアントに統合され、これにより AnyConnect クライアントは、ASA へのリモートアクセス接続を確立する前にポスチャアセスメントのクレデンシャルを収集できるようになります。
- ISE ポスチャ：OPSWAT v3 ライブラリを使用してポスチャ チェックを実行し、エンドポイントの適合性を評価します。その後、エンドポイントが適合するまでネットワーク アクセスを制限したり、ローカル ユーザーの権限を強化したりできます。
- AMP イネーブラ：エンドポイント向けの高度なマルウェア防御 (AMP) を導入する手段として使用されます。社内でローカルにホストされているサーバーからエンドポイントのサブセットに AMP for Endpoints ソフトウェアをプッシュし、既存のユーザーベースに AMP サービスをインストールします。
- ネットワーク可視性モジュール：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。NVM (ネットワーク可視性モジュール) は、エンドポイントのテレメトリを収集して、フローデータとファイルレピュテーションを syslog に記録し、さらに、ファイルの分析と UI インターフェイスの提供を行うコレクタ (サードパーティベンダー) にもフロー レコードをエクスポートします。
- Umbrella Roaming Security モジュール：アクティブな VPN がないときに DNS レイヤセキュリティを提供します。Cisco Umbrella Roaming と OpenDNS Umbrella サービスのいずれかに対するサブスクリプションを提供し、Intelligent Proxy および IP レイヤ適用機能を追加します。Umbrella Security Roaming プロファイルは、対応するサービスと各展開を関連付けて、対応する保護レベルを自動的に有効にします (コンテンツ

フィルタリング、複数のポリシー、強力なレポート、Active Directory 統合、または基本的な DNS レイヤ セキュリティ)。

- **Always-On VPN** : AnyConnect クライアント サービスプロファイルの常時接続 VPN フラグ設定をディセーブルにするか、または AnyConnect クライアント サービスプロファイル設定を使用する必要があるかを決定します。常時接続 VPN 機能により、ユーザーがコンピュータにログオンすると、AnyConnect は VPN セッションを自動的に確立します。VPN セッションは、ユーザーがコンピュータからログオフするまで維持されます。物理的な接続が失われてもセッションは維持され、AnyConnect クライアントは、適応型セキュリティアプライアンスとの物理的な接続の再確立を絶えず試行し、VPN セッションを再開します。

常時接続 VPN によって、企業ポリシーを適用して、セキュリティ脅威からデバイスを保護できます。常時接続 VPN を使用して、エンドポイントが信頼ネットワーク内ではない場合にいつでも AnyConnect クライアント が VPN セッションを確立したことを確認できます。イネーブルにすると、接続が存在しない場合のネットワーク接続の管理方法を決定するポリシーが設定されます。



(注) また、常時接続 VPN には AnyConnect セキュアモビリティ機能をサポートする AnyConnect クライアント リリースが必要です。

- [ダウンロードするクライアントプロファイル (Client Profiles to Download)] : プロファイルはコンフィギュレーションパラメータのグループであり、AnyConnect クライアントで VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ISE ポスチャ、AMP イネーブラ、ネットワーク可視性モジュール、および Umbrella Roaming Security モジュールの設定に使用されます。[追加 (Add)] をクリックして [AnyConnect クライアントプロファイルの選択 (Select Profiles)] ウィンドウを起動すると、以前グループポリシー用に作成されたプロファイルを指定できます。

内部グループポリシー、AnyConnect クライアント ログイン設定

内部グループポリシーの **Advanced** > AnyConnect クライアント > **Login Setting** ペインでは、リモートユーザーに AnyConnect クライアントのダウンロードを求めるプロンプトを表示したり、クライアントレス SSL VPN のポータルページにダイレクト接続するように ASA を設定できます。

- [Post Login Setting] : ユーザーにプロンプトを表示して、デフォルトのポスト ログイン選択を実行するためのタイムアウトを設定する場合に選択します。
- [Default Post Login Selection] : ログイン後に実行するアクションを選択します。

クライアント ファイアウォールによる VPN でのローカル デバイス サポートの有効化

内部グループポリシーの [詳細設定 (Advanced)] > [AnyConnect クライアント] > [クライアントファイアウォール (Client Firewall)] ペインでは、クライアントでのパブリックネットワー

クとプライベートネットワークの処理に影響するクライアントシステムのファイアウォールに送信するルールを設定できます。

リモートユーザーが ASA に接続すると、すべてのトラフィックがその VPN 接続を介してトンネリングされるため、ユーザーはローカルネットワーク上のリソースにアクセスできなくなります。こうしたリソースには、ローカルコンピュータと同期するプリンタ、カメラ、Windows Mobile デバイス（テザー デバイス）などが含まれます。この問題は、クライアントプロファイルで [Local LAN Access] を有効にすることで解消されます。ただし、ローカルネットワークへのアクセスが無制限になるため、一部の企業ではセキュリティやポリシーについて懸念が生じる可能性があります。プリンタやテザー デバイスなど特定タイプのローカルリソースに対するアクセスを制限するエンドポイントの OS のファイアウォールルールを導入するように ASA を設定できます。

そのための操作として、印刷用の特定ポートに対するクライアントファイアウォールルールを有効にします。クライアントでは、着信ルールと発信ルールが区別されます。印刷機能の場合、クライアントでは発信接続に必要なポートは開放されますが、着信トラフィックはすべてブロックされます。



- (注) 管理者としてログインしたユーザーは、ASA によりクライアントへ展開されたファイアウォールルールを修正できることに注意が必要です。限定的な権限を持つユーザーは、ルールを修正できません。どちらのユーザーの場合も、接続が終了した時点でクライアントによりファイアウォールルールが再適用されます。

クライアントファイアウォールを設定している場合、ユーザーが Active Directory (AD) サーバーで認証されると、クライアントでは引き続き ASA のファイアウォールポリシーが適用されます。ただし、AD グループポリシーで定義されたルールは、クライアントファイアウォールのルールよりも優先されます。

ASA でクライアントファイアウォールルールが設定され、エンドポイントで VPN 接続が確立されている場合、

- ASA は、ファイアウォールルール情報をクライアントに送信します。
- クライアントは、必要に応じてファイアウォールルールを適用します。

以下の項では、次の処理を行うための手順について説明します。

- [ローカルプリンタをサポートするためのクライアントファイアウォールの展開 \(37 ページ\)](#)
- [VPN のテザー デバイス サポートの設定 \(40 ページ\)](#)

ファイアウォールの動作に関する注意事項

以下は、AnyConnect クライアント でのファイアウォールの使用方法に関する注意事項です。

- ファイアウォールルールには送信元 IP は使用されません。クライアントでは、ASA から送信されたファイアウォールルール内の送信元 IP 情報は無視されます。送信元 IP は、

ルールがパブリックかプライベートかに応じてクライアントが特定します。パブリックルールは、クライアント上のすべてのインターフェイスに適用されます。プライベートルールは、仮想アダプタに適用されます。

- ASA は、ACL ルールに対して数多くのプロトコルをサポートしています。ただし、AnyConnect クライアントのファイアウォール機能でサポートされているのは、TCP、UDP、ICMP、および IP のみです。クライアントでは、異なるプロトコルでルールが受信された場合、そのルールは無効なファイアウォールルールとして処理され、さらにセキュリティ上の理由からスプリット トンネリングが無効となり、フル トンネリングが使用されます。
- ASA 9.0 から、パブリック ネットワーク ルールおよびプライベート ネットワーク ルールは、ユニファイド アクセス コントロール リストをサポートしています。これらのアクセス コントロール リストは、同じルールで IPv4 および IPv6 トラフィックを定義する場合に使用できます。

ただし次のように、オペレーティング システムによって動作が異なるため注意が必要です。

- Windows コンピュータの場合、Windows Firewall では拒否ルールが許可ルールに優先します。ASA により許可ルールが AnyConnect クライアントにプッシュされても、ユーザーがカスタムの拒否ルールを作成している場合、AnyConnect クライアントルールは適用されません。
- Windows Vista の場合、ファイアウォールルールが作成されると、Windows Vista ではポート番号の範囲がカンマ区切りの文字列として認識されます。ポート範囲は、最大で 300 ポートです (1 ~ 300、5000 ~ 5300 など)。指定した範囲が 300 ポートを超える場合は、最初の 300 ポートに対してのみファイアウォールルールが適用されます。
- ファイアウォールサービスが AnyConnect クライアントにより開始される必要がある (システムにより自動的に開始されない) Windows ユーザーは、VPN 接続の確立時間が大幅に増える場合があります。
- Mac コンピュータの場合、AnyConnect クライアントでは、ASA で適用された順序と同じ順序でルールが適用されます。グローバルルールは必ず最後になるようにしてください。
- サードパーティ ファイアウォールの場合、AnyConnect クライアント ファイアウォールとサードパーティファイアウォールの両方で許可されているトラフィックタイプのトラフィックのみ通過できます。AnyConnect クライアントで許可されている特定のトラフィックタイプがサードパーティファイアウォールでブロックされる場合、そのタイプのトラフィックはクライアントでブロックされます。

ローカル プリンタをサポートするためのクライアント ファイアウォールの展開

ASA は、ASA バージョン 8.3(1) 以降および ASDM バージョン 6.3(1) 以降で、AnyConnect クライアント ファイアウォール機能をサポートします。この項では、ローカル プリンタへのアクセスが許可されるようにクライアント ファイアウォールを設定する方法、および VPN 接続の失敗時にファイアウォールを使用するようクライアント プロファイルを設定する方法について説明します。

クライアントファイアウォールの制限事項

クライアントファイアウォールを使用してローカル LAN アクセスを制限する場合には次の制限事項が適用されます。

- `deny ip any any` プライベートルールは許可されません。
- OS の制限事項により、Windows XP が実行されているコンピュータのクライアントファイアウォールポリシーは、着信トラフィックに対してのみ適用されます。発信ルールおよび双方向ルールは無視されます。これには、「`permit ip any any`」などのファイアウォールルールが含まれます。
- HostScan（現在の名前は Secure Firewall Posture）や一部のサードパーティファイアウォールは、ファイアウォールを妨害する可能性があります。

以下の表は、送信元ポートおよび宛先ポートの設定により影響を受けるトラフィックの方向をまとめたものです。

送信元ポート (Source Port)	接続先ポート	影響を受けるトラフィックの方向
特定のポート番号	特定のポート番号	着信および発信
範囲または「すべて」（値は 0）	範囲または「すべて」（値は 0）	着信および発信
特定のポート番号	範囲または「すべて」（値は 0）	着信のみ
範囲または「すべて」（値は 0）	特定のポート番号	発信のみ

ローカル印刷に関する ACL ルールの例

ACL AnyConnect クライアント_Local_Print は、クライアントファイアウォールを設定しやすくするために、ASDM を備えています。グループポリシーの [Client Firewall] ペインのパブリック ネットワーク ルールのために ACL を選択する際は、一覧に次の ACE を含めます。

表 1: AnyConnect クライアント_Local_Print の ACL ルール

説明	権限	インターフェイス	プロトコル	送信元ポート	宛先アドレス	宛先ポート
すべて拒否	拒否	パブリック	いずれか (Any)	デフォルト	いずれか (Any)	デフォルト

説明	権限	インターフェイス	プロトコル	送信元ポート	宛先アドレス	宛先ポート
LPD	許可	パブリック	TCP	デフォルト	いずれか (Any)	515
IPP	許可	パブリック	TCP	デフォルト	いずれか (Any)	631
プリンタ	許可	パブリック	TCP	デフォルト	いずれか (Any)	9100
mDNS	許可	パブリック	UDP	デフォルト	224.0.0.251	5353
LLMNR	許可	パブリック	UDP	デフォルト	224.0.0.252	5355
NetBios	許可	パブリック	TCP	デフォルト	いずれか (Any)	137
NetBios	許可	パブリック	UDP	デフォルト	いずれか (Any)	137
(注) デフォルトのポート範囲は 1 ~ 65535 です。						



(注) ローカル印刷を有効にするには、定義済み ACL ルール「allow Any Any」に対し、クライアントプロファイルの [Local LAN Access] 機能を有効にする必要があります。

VPN のローカル印刷サポートの設定

エンドユーザーがローカルプリンタに出力できるようにするには、グループポリシーで標準 ACL を作成します。ASA はその ACL を VPN クライアントに送信し、VPN クライアントはクライアントのファイアウォール設定を変更します。

手順

- ステップ 1** グループポリシーで、AnyConnect クライアントファイアウォールを有効にします。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。
- ステップ 2** グループポリシーを選択して、[Edit] をクリックします。
- ステップ 3** [詳細設定 (Advanced)] > [AnyConnect クライアント] > [クライアントファイアウォール (Client Firewall)] を選択します。プライベート ネットワーク ルールに対応する [Manage] をクリックします。

- ステップ 4** 前述した ACE を含む ACL を作成します。この ACL をプライベート ネットワーク ルールとして追加します。
- ステップ 5** 常時接続の自動 VPN ポリシーを有効にし、かつクローズドポリシーを指定している場合、VPN 障害が発生するとユーザーはローカルリソースにアクセスできません。このシナリオでは、プロファイルエディタの [Preferences (Part 2)] に移動し、[Apply last local VPN resource rules] をオンにすることによって、ファイアウォールルールを適用できます。

VPN のテザー デバイス サポートの設定

テザー デバイスをサポートして企業ネットワークを保護する場合は、グループ ポリシーで標準的な ACL を作成し、テザーデバイスで使用する宛先アドレスの範囲を指定します。さらに、トンネリング VPN トラフィックから除外するネットワーク リストとしてスプリット トンネリング用の ACL を指定します。また、VPN 障害時には最後の VPN ローカル リソース ルールが使用されるようにクライアント プロファイルを設定することも必要です。



- (注) AnyConnect クライアント を実行するコンピュータと同期する必要がある Windows モバイルデバイスについては、ACL で IPv4 宛先アドレスを 169.254.0.0、または IPv6 宛先アドレスを fe80::/64 と指定します。

手順

- ステップ 1** ASDM で、[Group Policy] > [Advanced] > [Split Tunneling] を選択します。
- ステップ 2** [Network List] フィールドの隣にある [Inherit] チェックボックスをオフにし、[Manage] をクリックします。
- ステップ 3** [Extended ACL] タブをクリックします。
- ステップ 4** [Add] > [Add ACL] を選択します。新しい ACL の名前を指定します。
- ステップ 5** テーブルで新しい ACL を選択して、[Add] をクリックし、さらに [Add ACE] をクリックします。
- ステップ 6** [Action] に対して [Permit] オプション ボタンを選択します。
- ステップ 7** 宛先条件エリアで、IPv4 宛先アドレスを 169.254.0.0、または IPv6 宛先アドレスを fe80::/64 と指定します。
- ステップ 8** [Service] に対して IP を選択します。
- ステップ 9** [OK] をクリックします。
- ステップ 10** [OK] をクリックして、ACL を保存します。
- ステップ 11** 内部グループ ポリシーの [Split Tunneling] ペインで、ステップ 7 で指定した IP アドレスに応じて [Inherit for the Policy or IPv6 Policy] チェックボックスをオフにして、[Exclude Network List Below] を選択します。[Network List] で、作成した ACL を選択します。
- ステップ 12** [OK] をクリックします。

ステップ 13 [Apply] をクリックします。

内部グループポリシー、AnyConnect クライアント キーの再生成

ASA とクライアントがキーを再生成し、暗号キーと初期ベクトルについて再ネゴシエーションするときに、キー再生成ネゴシエーションが実行され、接続のセキュリティが強化されます。

内部グループポリシーの [詳細設定 (Advanced)] > [AnyConnect クライアント] > [キーの再生成 (Key Regeneration)] ペインでは、キー再生成のパラメータを設定します。

- [Renegotiation Interval] : セッションの開始からキーの再生成が実行されるまでの分数を 1 ~ 10080 (1 週間) の範囲で指定するには、[Unlimited] チェックボックスをオフにします。
- [Renegotiation Method] : [Inherit] チェックボックスをオフにして、デフォルトのグループポリシーとは異なる再ネゴシエーション方式を指定します。キー再生成をディセーブルにするには、[None] オプション ボタンを選択し、キー再生成時に新しいトンネルを確立するには、[SSL] または [New Tunnel] オプション ボタンを選択します。



(注) [Renegotiation Method] を [SSL] または [New Tunnel] に設定すると、キー再生成時に SSL 再ネゴシエーションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されます。anyconnect ssl rekey コマンドの履歴については、コマンドリファレンスを参照してください。

内部グループポリシー、AnyConnect クライアント、デッドピア検出

Dead Peer Detection (DPD) により、ピアの応答がなく接続が失敗している場合には、ASA (ゲートウェイ) またはクライアント側で瞬時に検出できます。デッドピア検出 (DPD) を有効にし、AnyConnect クライアントまたは ASA ゲートウェイが DPD を実行する頻度を設定するには、以下の手順を実行します。

始める前に

- この機能は、ASA ゲートウェイと AnyConnect クライアント SSL VPN クライアント間の接続のみに適用されます。DPD は、埋め込みが許可されない標準実装に基づくため、IPsec とは併用できません。
- DTLS をイネーブルにすると、Dead Peer Detection (DPD) もイネーブルになります。DPD により、失敗した DTLS 接続の TLS へのフォールバックがイネーブルになります。それ以外の場合、接続は終了します。
- ASA で DPD が有効になっているとき、Optimal MTU (OMTU) 機能を使用すると、クライアントが DTLS パケットを正常に渡すことができる最大のエンドポイント MTU を見つけることができます。最大 MTU までパディングされた DPD パケットを送信することによって、OMTU を実装します。ペイロードの正しいエコーをヘッドエンドから受信する

と、MTU サイズが受け入れられます。受け入れられなかった場合、MTU は小さくされ、プロトコルで許可されている最小 MTU に到達するまで、繰り返しプローブが送信されます。

手順

ステップ 1 目的のグループ ポリシーに移動します。

- [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [グループポリシー (Group Policies)] の順に移動し、目的のグループ ポリシーを追加 ([追加 (Add)]) または編集 ([編集 (Edit)]) し、[詳細設定 (Advanced)] > [AnyConnect クライアント] > [デッドピア検出 (Dead Peer Detection)] ペインを開きます。
- または特定のユーザーポリシーに到達するには、[設定 (Configuration)] > [デバイス管理 (Device Management)] > [ユーザー/AAA (Users/AAA)] > [ユーザーアカウント (User Accounts)] に移動し、目的のユーザーアカウントを追加 ([追加 (Add)]) または編集 ([編集 (Edit)]) し、[VPN ポリシー (VPN Policy)] > [AnyConnect クライアント] > [デッドピア検出 (Dead Peer Detection)] ペインを開きます。

ステップ 2 ゲートウェイ側の検出を設定します。

DPD をセキュリティアプライアンス (ゲートウェイ) によって実行することを指定するには、[Disable] チェックボックスをオフにします。セキュリティアプライアンスが DPD を実行する間隔を 30 秒 (デフォルト) から 3600 秒の範囲で入力します。値 300 が推奨されます。

ステップ 3 クライアント側の検出を設定します。

DPD をクライアントが実行することを指定するには、[Disable] チェックボックスをオフにします。クライアントが DPD を実行する間隔を 30 秒 (デフォルト) から 3600 秒の範囲で入力します。30 秒が推奨されます。

内部グループポリシー、クライアントレスポータルの AnyConnect クライアント カスタマイズ

内部グループポリシーの [詳細設定 (Advanced)] > [AnyConnect クライアント] > [カスタマイズ (Customization)] ペインでは、グループポリシーのクライアントレスポータルのログインページをカスタマイズできます。

- [ポータルのカスタマイズ (Portal Customization)] : [AnyConnect クライアント/SSL VPN] ポータルページに適用するカスタマイゼーションを選択します。事前設定済みのポータルカスタマイゼーション オブジェクトを選択するか、またはデフォルト グループ ポリシーで定義されているカスタマイゼーションを受け入れることができます。デフォルトは DfltCustomization です。

- **[Manage]** : **[Configure GUI Customization object]**s ダイアログボックスが開きます。このダイアログボックスでは、カスタマイゼーションオブジェクトの追加、編集、削除、インポート、またはエクスポートを指定できます。
- **[Homepage URL]**(オプション) : グループポリシーに関連付けられたユーザーのクライアントレスポータルに表示するホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。認証に成功すると、クライアントレスポータルにはすぐにこのページが表示されます。VPN 接続が正常に確立されると、AnyConnect クライアントによってデフォルトの Web ブラウザが起動され、この URL が表示されます。



(注) AnyConnect クライアントは、Linux プラットフォーム、Android モバイルデバイス、および Apple iOS モバイルデバイスでこのフィールドを現在サポートしていません。設定されている場合、これらの AnyConnect クライアントは無視されます。

- **[Use Smart Tunnel for Homepage]** : ポート転送を使用する代わりにポータルに接続するスマートトンネルを作成します。
- **[Access Deny Message]** : アクセスを拒否するユーザーに表示するメッセージを作成するには、このフィールドに入力します。

内部グループポリシーの AnyConnect クライアントカスタム属性の設定

内部グループポリシーの [詳細設定 (Advanced)] > [AnyConnect クライアント] > [カスタム属性 (Custom Attributes)] ペインは、このポリシーに現在割り当てられているカスタム属性を示します。このダイアログボックスでは、すでに定義済みのカスタム属性をこのポリシーに関連付けるか、カスタム属性を定義してこのポリシーに関連付けることができます。

カスタム属性は AnyConnect クライアントに送信され、アップグレードの延期などの機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。まず属性のタイプを定義した後、このタイプの名前付きの値を1つ以上定義できます。機能に対して設定する固有のカスタム属性の詳細については、使用している AnyConnect クライアントリリースの『Cisco Secure Client Administrator Guide』を参照してください。

カスタム属性は、[設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [詳細設定 (Advanced)] > [AnyConnect クライアントカスタム属性 (Custom Attributes)] および [AnyConnect クライアントカスタム属性名 (Custom Attribute Names)] で事前に定義することもできます。事前に定義したカスタム属性は、ダイナミックアクセスポリシーとグループポリシーの両方で使用されます。

この手順を使用して、カスタム属性を追加または編集します。設定済みのカスタム属性を削除することもできますが、別のグループポリシーに関連付けられている場合は編集または削除できません。

手順

-
- ステップ 1** [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [グループポリシー (Group Policies)] > [追加/編集 (Add/Edit)] > [詳細設定 (Advanced)] > [AnyConnect クライアント] > [カスタム属性 (Custom Attributes)] に移動します。
- ステップ 2** [Add] をクリックして [Create Custom Attribute] ペインを開きます。
- ステップ 3** ドロップダウンリストから事前に定義された属性タイプを選択するか、次の手順を実行して属性タイプを設定します。
- [管理 (Manage)] をクリックし、[カスタム属性タイプの設定 (Configure Custom Attribute Types)] ペインで [追加 (Add)] をクリックします。
 - [カスタム属性タイプの作成 (Create Custom Attribute Type)] ペインで、新しい属性の [タイプ (Type)] と [説明 (Description)] を入力します。どちらのフィールドも必須項目です。AnyConnect クライアント カスタム属性オプションについては、[AnyConnect クライアント カスタム属性 \(118 ページ\)](#) を参照してください。
 - [OK] をクリックしてこのペインを閉じ、もう一度 [OK] をクリックして、新しく定義したカスタム属性のタイプを選択します。
- ステップ 4** [値の選択 (Select Value)] を選択します。
- ステップ 5** [値の選択 (Select value)] ドロップダウンリストから事前に定義された名前付きの値を選択するか、次の手順を実行して新しい名前付きの値を設定します。
- [管理 (Manage)] をクリックし、[カスタム属性の設定 (Configure Custom Attributes)] ペインで [追加 (Add)] をクリックします。
 - [カスタム属性名の作成 (Create Custom Attribute Name)] ペインで、前に選択または設定した属性タイプを選択し、新しい属性の [名前 (Name)] と [値 (Value)] を入力します。どちらのフィールドも必須項目です。
- 値を追加するには、[追加 (Add)] をクリックして値を入力し、[OK] をクリックします。値は 420 文字を超えてはなりません。値がこの長さを超える場合は、追加の値コンテンツの複数の値を追加します。設定値は AnyConnect クライアント に送信される前に連結されます。
- [OK] をクリックしてこのペインを閉じ、もう一度 [OK] をクリックして、この属性の新しく定義した名前付きの値を選択します。
- ステップ 6** [カスタム属性の作成 (Create Custom Attribute)] ペインで [OK] をクリックします。
-

IPsec (IKEv1) クライアントの内部グループポリシー

内部グループポリシー、IPsec (IKEv1) クライアントの一般属性

[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] で、[Add or Edit Group Policy] > [IPsec] ダイアログボックスを使用すると、

追加または変更するグループポリシーのトンネリングプロトコル、フィルタ、接続設定、サーバーを指定できます。

- [Re-Authentication on IKE Re-key] : [Inherit] チェックボックスがオフである場合に、IKE キーの再生成が行われたときの再認証をイネーブルまたはディセーブルにします。ユーザーは、30 秒以内にクレデンシャルを入力する必要があります。また、約 2 分間で SA が期限切れになり、トンネルが終了するまでの間に、3 回まで入力を再試行できます。
- [Allow entry of authentication credentials until SA expires] : 設定済み SA の最大ライフタイムまで、ユーザーは認証クレデンシャルをこの回数再入力できます。
- [IP Compression] : [Inherit] チェックボックスがオフである場合に、IP Compression をイネーブルまたはディセーブルにします。
- [Perfect Forward Secrecy] : [Inherit] チェックボックスがオフである場合に、完全転送秘密 (PFS) をイネーブルまたはディセーブルにします。PFS は、特定の IPsec SA のキーが他のシークレット (他のキーなど) から導出されたものでないことを保証します。つまり、PFS では、攻撃者があるキーを突破しても、そこから他のキーを導出することはできないことが保証されます。PFS がイネーブルになっていない場合は、IKE SA の秘密キーが突破されると、その攻撃者は、IPsec のすべての保護データをコピーし、IKE SA のシークレットの知識を使用して、その IKE SA によって設定された IPsec SA のセキュリティを侵すことができると推測されます。PFS を使用すると、攻撃者が IKE を突破しても、直接 IPsec にはアクセスできません。その場合、攻撃者は各 IPsec SA を個別に突破する必要があります。
- [Store Password on Client System] : クライアントシステムでのパスワードの保管をイネーブルまたはディセーブルにします。



(注) パスワードをクライアントシステムで保管すると、潜在的なセキュリティ リスクが発生します。

- [IPsec over UDP] : IPsec over UDP の使用をイネーブルまたはディセーブルにします。
- [IPsec over UDP Port] : IPsec over UDP で使用する UDP ポートを指定します。
- [Tunnel Group Lock] : [Inherit] チェックボックスまたは値 [None] が選択されていない場合に、選択したトンネルグループをロックします。
- [IPsec Backup Servers] : [Server Configuration] フィールドと [Server IP Addresses] フィールドをアクティブにします。これによって、これらの値が継承されない場合に使用する UDP バックアップサーバーを指定できます。
 - [Server Configuration] : IPsec バックアップサーバーとして使用するサーバー設定オプションを一覧表示します。使用できるオプションは、[Keep Client Configuration] (デフォルト)、[Use Backup Servers Below]、および [Clear Client Configuration] です。

- [Server Addresses (space delimited)] : IPsec バックアップ サーバーの IP アドレスを指定します。このフィールドは、[Server Configuration] で選択した値が Use Backup Servers Below である場合にだけ使用できます。

内部グループポリシーの IPsec (IKEv1) クライアントのアクセスルールについて

このダイアログボックスの [Client Access Rules] テーブルには、クライアントアクセスルールを 25 件まで表示できます。クライアントアクセスルールを追加するときには次のフィールドを設定します。

- [Priority] : このルールの優先順位を選択します。
- [Action] : このルールに基づいてアクセスを許可または拒否します。
- [VPN Client Type] : このルールを適用する VPN クライアントのタイプ (ソフトウェアまたはハードウェア) を指定します。ソフトウェアクライアントの場合は、すべての Windows クライアントまたはサブセットを自由形式のテキストで指定します。
- [VPN Client Version] : このルールを適用する VPN クライアントのバージョンを指定します (複数可)。このカラムには、このクライアントに適用されるソフトウェアまたはファームウェア イメージのカンマ区切りリストが含まれます。エントリは自由形式のテキストで、* はすべてのバージョンと一致します。

クライアントアクセスルールの定義

- ルールを定義しない場合、ASA はすべての接続タイプを許可します。ただし、ユーザーがデフォルトグループポリシーに存在するルールを継承する場合があります。
- クライアントがいずれのルールにも一致しない場合、ASA は接続を拒否します。拒否ルールを定義する場合は、許可ルールも 1 つ以上定義する必要があります。許可ルールを定義しないと、ASA はすべての接続を拒否します。
- * 文字はワイルドカードです。ワイルドカードは各ルールで複数回入力することができます。
- ルールセット全体に対して 255 文字の制限があります。
- クライアントのタイプまたはバージョン (あるいはその両方) を送信しないクライアントには、**n/a** を入力できます。

内部グループポリシー、IPsec (IKEv1) クライアントのクライアントファイアウォール

[Add or Edit Group Policy] の [Client Firewall] ダイアログボックスでは、追加または変更するグループポリシーに対して VPN クライアントのファイアウォール設定を行うことができます。これらのファイアウォール機能を使用できるのは、Microsoft Windows 上で動作している VPN クライアントだけです。現在、ハードウェアクライアントまたは他 (Windows 以外) のソフトウェアクライアントでは、これらの機能は使用できません。

VPNクライアントを使用してASAに接続しているリモートユーザーは、適切なファイアウォール オプションを選択できます。

最初のシナリオでは、リモートユーザーのPC上にパーソナルファイアウォールがインストールされています。VPNクライアントは、ローカルファイアウォールで定義されているファイアウォールポリシーを適用し、そのファイアウォールが実行されていることを確認するためにモニターします。ファイアウォールの実行が停止すると、VPNクライアントはASAへの通信をドロップします（このファイアウォール適用メカニズムはAre You There (AYT) と呼ばれます。VPNクライアントが定期的に「are you there?」メッセージを送信することによってファイアウォールをモニターするからです。応答が返されない場合、VPNクライアントは、ファイアウォールがダウンしたためASAへの接続が終了したと認識します。）ネットワーク管理者がこれらのPCファイアウォールを独自に設定する場合がありますが、この方法を使用すれば、ユーザーは各自の設定をカスタマイズできます。

第2のシナリオでは、VPNクライアントPCのパーソナルファイアウォールに中央集中型ファイアウォールポリシーを適用することが選択されることがあります。一般的な例としては、スプリットトンネリングを使用してグループのリモートPCへのインターネットトラフィックをブロックすることが挙げられます。この方法は、トンネルが確立されている間、インターネット経由の侵入からPCを保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、プッシュポリシーまたはCentral Protection Policy (CPP) と呼ばれます。ASAでは、VPNクライアントに適用するトラフィック管理ルールのセットを作成し、これらのルールをフィルタに関連付けて、そのフィルタをファイアウォールポリシーとして指定します。ASAはこのポリシーをVPNクライアントまで配信します。その後、VPNクライアントはポリシーをローカルファイアウォールに渡し、そこでポリシーが適用されます。

[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] > [Client Firewall]

フィールド

- [Inherit] : グループポリシーがデフォルトグループポリシーからクライアントのファイアウォール設定を取得するかどうかを決めます。このオプションはデフォルト設定です。設定すると、このダイアログボックスにある残りの属性がその設定によって上書きされ、名前がグレー表示になります。
- [Client Firewall Attributes] : (実装されている場合) 実装されているファイアウォールのタイプやファイアウォールポリシーなど、クライアントのファイアウォール属性を指定します。
- [Firewall Setting] : ファイアウォールが存在するかどうかを一覧表示します。存在する場合には、そのファイアウォールが必須かオプションかも示します。[No Firewall] (デフォルト) を選択すると、このダイアログボックスにある残りのフィールドは、いずれもアクティブになりません。このグループのユーザーをファイアウォールで保護する場合は [Firewall Required] または [Firewall Optional] 設定を選択します。

[Firewall Required] を選択した場合は、このグループのユーザー全員が指定されたファイアウォールを使用する必要があります。指定されたサポート対象のファイアウォールがインストールされておらず、実行されていない場合、ASAは接続を試行したセッションをすべ

てドロップします。この場合、ASA は、ファイアウォール設定が一致しないことを VPN クライアントに通知します。



- (注) グループでファイアウォールを必須にする場合には、そのグループに Windows VPN クライアント以外のクライアントが存在しないことを確認してください。グループ内のその他のクライアント (クライアントモードの ASA 5505 を含む) は接続できません。

このグループに、まだファイアウォールに対応していないリモートユーザーがいる場合は、[Firewall Optional] を選択します。Firewall Optional 設定を使用すると、グループ内のすべてのユーザーが接続できるようになります。ファイアウォールに対応しているユーザーは、ファイアウォールを使用できます。ファイアウォールなしで接続するユーザーには、警告メッセージが表示されます。この設定は、一部のユーザーがファイアウォールをサポートしており、他のユーザーがサポートしていないグループを作成するときに役立ちます。たとえば、移行途中のグループでは、一部のメンバはファイアウォール機能を設定し、別のユーザーはまだ設定していないことがあります。

- [Firewall Type] : シスコを含む複数のベンダーのファイアウォールを一覧表示します。[Custom Firewall] を選択すると、[Custom Firewall] の下のフィールドがアクティブになります。指定したファイアウォールが、使用できるファイアウォールポリシーと関連している必要があります。設定したファイアウォールにより、サポートされるファイアウォールポリシー オプションが決まります。
- [Custom Firewall] : カスタムファイアウォールのベンダーID、製品ID、および説明を指定します。
 - [Vendor ID] : このグループポリシーのカスタムファイアウォールのベンダーを指定します。
 - [Product ID] : このグループポリシー用に設定するカスタムファイアウォールの製品名またはモデル名を指定します。
 - [Description] : (任意) カスタムファイアウォールについて説明します。
- [Firewall Policy] : カスタムファイアウォールポリシーのタイプとソースを指定します。
 - [Policy defined by remote firewall (AYT)] : ファイアウォールポリシーをリモートファイアウォール (Are You There) によって定義するように指定します。Policy defined by remote firewall (AYT) は、このグループのリモートユーザーのファイアウォールが、各自の PC に存在することを意味しています。このローカルファイアウォールが、VPN クライアントにファイアウォールポリシーを適用します。ASA は、指定されたファイアウォールがインストールされ、実行している場合にのみ、このグループのVPNクライアントが接続できるようにします。指定されたファイアウォールが実行されていない場合、接続は失敗します。接続が確立すると、VPNクライアントがファイアウォールを30秒ごとにポーリングして、そのファイアウォールが実行されている

ことを確認します。ファイアウォールの実行が停止すると、VPNクライアントはセッションを終了します。

- **[Policy pushed (CPP)]** : ポリシーがピアからプッシュされるように指定します。このオプションを選択する場合は、**[Inbound Traffic Policy]** および **[Outbound Traffic Policy]** リストと **[Manage]** ボタンがアクティブになります。ASA は、**[Policy Pushed (CPP)]** ドロップダウンリストで選択されたフィルタによって定義されるトラフィック管理ルールを、このグループのVPNクライアントに適用します。メニューで選択できるのは、デフォルトフィルタを含めて、このASAで定義されているフィルタです。ASAがこれらのルールをVPNクライアントにプッシュすることに注意してください。ASAではなくVPNクライアントに対してこれらのルールを作成して定義する必要があります。たとえば、「in」と「out」はそれぞれ、VPNクライアントに着信するトラフィックと、VPNクライアントから発信されるトラフィックです。VPNクライアントにローカルファイアウォールもある場合、ASAからプッシュされたポリシーはローカルファイアウォールのポリシーと連携して機能します。いずれかのファイアウォールのルールでブロックされたすべてのパケットがドロップされます。
- **[Inbound Traffic Policy]** : 着信トラフィックに対して使用できるプッシュポリシーを一覧表示します。
- **[Outbound Traffic Policy]** : 発信トラフィックに対して使用できるプッシュポリシーを一覧表示します。
- **[Manage]** : **[ACL Manager]** ダイアログボックスを表示します。このダイアログボックスで、アクセスコントロールリスト (ACL) を設定できます。

サイト間内部グループポリシー

サイト間VPN接続のグループポリシーでは、トンネリングプロトコル、フィルタ、および接続設定を指定します。このダイアログボックスの各フィールドで、**[Inherit]** チェックボックスを選択すると、対応する設定の値をデフォルトグループポリシーから取得できます。**[Inherit]** は、このダイアログボックスの属性すべてのデフォルト値です。

フィールド

[Add Internal Group Policy] > [General] ダイアログボックスには、次の属性が表示されます。これらの属性は、SSL VPN と IPsec セッションに適用されます。そのため、いくつかの属性は、1つのタイプのセッションに表示され、他のタイプには表示されません。

- **[Name]** : このグループポリシーの名前を指定します。Edit機能の場合、このフィールドは読み取り専用です。
- **[Tunneling Protocols]** : このグループが許可するトンネリングプロトコルを指定します。ユーザーは、選択されているプロトコルだけを使用できます。次の選択肢があります。
- **[Clientless SSL VPN]** : SSL VPN (SSL/TLS を利用する VPN) を使用することを指定します。このVPNでは、ソフトウェアやハードウェアのクライアントは必要なく、Webブラウザを使用してASAへのセキュアなリモートアクセストンネルが確立されます。

クライアントレス SSL VPN を使用すると、HTTPS インターネットサイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベースアプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。

- [SSL VPN クライアント (SSL VPN Client)] : Cisco AnyConnect VPN Client またはレガシー SSL VPN クライアントの AnyConnect VPN モジュールの使用を指定します。AnyConnect クライアントを使用している場合は、このプロトコルを選択して MUS がサポートされるようにする必要があります。
- [IPsec IKEv1] : IP セキュリティプロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site (ピアツーピア) 接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2] : Secure Client によってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect クライアント接続では、ソフトウェアアップデート、クライアントプロファイル、GUI のローカリゼーション (翻訳) とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- [L2TP over IPsec] : 一部の一般的な PC やモバイル PC のオペレーティングシステムで提供される VPN クライアントを使用しているリモートユーザーは、L2TP over IPsec によって、パブリック IP ネットワーク経由でセキュリティアプライアンスやプライベート企業ネットワークへのセキュアな接続を確立できます。L2TP は、データのトンネリングに PPP over UDP (ポート 1701) を使用します。セキュリティアプライアンスは、IPsec 転送モード用に設定する必要があります。
- [フィルター (Filter)] : (Network (Client) Access 専用) 使用するアクセスコントロールリストを指定するか、またはグループポリシーから値を継承するかどうかを指定します。フィルタは複数のルールから構成されています。これらのルールは、ASA を介して着信したトンネリングデータパケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。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。フィルタおよびルールを設定する方法については、[Group Policy] ダイアログボックスを参照してください。ACL を表示および設定できる [ACL Manager] を開くには、[Manage] をクリックします。
- Idle Timeout : [Inherit] チェックボックスをオフにした場合、このパラメータでアイドル時間を分単位で設定します。

この期間に接続で通信アクティビティがない場合、接続は終了します。最小時間は 1 分、最大時間は 10080 分であり、デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。
- Maximum Connect Time : [Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザー接続時間を分単位で設定します。

ここで指定した時間が経過すると、システムは接続を終了します。最小値は1分、最大値は35791394分です。制限なしの接続時間を許可するには、[Unlimited]をオンにします（デフォルト）。

- **Periodic Certificate Authentication Interval**：証明書認証が定期的に再実行されるまでの時間間隔（時間単位）。

[Inherit] チェックボックスがオフになっている場合、定期的な証明書検証の実行間隔を設定できます。範囲は1～168時間で、デフォルトは無効になっています。無制限の検証を許可するには、[Unlimited]をオンにします。

ローカルユーザーのVPNポリシー属性の設定

この手順では、既存のユーザーを編集する方法について説明します。ユーザーを追加するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択し、[Add] をクリックします。詳細については、一般的操作用コンフィギュレーションガイドを参照してください。

始める前に

デフォルトで、ユーザーアカウントはデフォルトグループポリシー DfltGrpPolicy から設定値を継承します。各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。

手順

- ステップ 1** ASDM を開始し、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] の順に選択します。
- ステップ 2** 設定するユーザーを選択し、[Edit] をクリックします。
- ステップ 3** 左側のペインで、[VPN Policy] をクリックします。
- ステップ 4** ユーザーのグループポリシーを指定します。ユーザーポリシーは、このグループポリシーの属性を継承します。この画面にデフォルトグループポリシーの設定を継承するよう設定されている他のフィールドがある場合、このグループポリシーで指定された属性がデフォルトグループポリシーで設定された属性より優先されます。
- ステップ 5** ユーザーが使用できるトンネリングプロトコルを指定するか、グループポリシーから値を継承するかどうかを指定します。

目的の [Tunneling Protocols] チェックボックスをオンにし、次のトンネリングプロトコルのいずれかを選択します。

- **SSL VPN クライアント**は、AnyConnect クライアントアプリケーションのダウンロード後にユーザーが接続できるようにします。ユーザーは、最初にクライアントレス SSL VPN 接続を使用してこのアプリケーションをダウンロードします。ユーザーが接続するたびに、必要に応じてクライアントアップデートが自動的に行われます。

- [IPsec IKEv1] : IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site (ピアツーピア) 接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
 - [IPsec IKEv2] : AnyConnect クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect クライアント 接続では、ソフトウェアアップデート、クライアントプロファイル、GUI のローカライゼーション (翻訳) とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
 - 一部の一般的 PC やモバイル PC のオペレーティングシステムで提供される VPN クライアントを使用しているリモートユーザーは、L2TP over IPsec によって、パブリック IP ネットワーク経由で ASA およびプライベート企業ネットワークへのセキュアな接続を確立できます。
- (注) プロトコルを選択しなかった場合は、エラーメッセージが表示されます。

ステップ 6 使用するフィルタ (IPv4 または IPv6) を指定するか、またはグループ ポリシーの値を継承するかどうかを指定します。

フィルタは複数のルールから構成されています。これらのルールは、ASA を介して着信したトンネリング データ パケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。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。

- a) フィルタとルールを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options] > [Filter] の順に選択します。
- b) [Manage] をクリックして、ACL と ACE を追加、編集、および削除できる [ACL Manager] ペインを表示します。

ステップ 7 接続プロファイル (トンネルグループロック) がある場合、それを継承するかどうか、または選択したトンネルグループロックを使用するかどうかを指定します。

特定のロックを選択すると、ユーザーのリモートアクセスはこのグループだけに制限されます。[Tunnel Group Lock] では、VPN クライアントで設定されたグループと、そのユーザーが割り当てられているグループが同じかどうかをチェックすることによって、ユーザーが制限されます。一致していない場合、ASA はユーザーが接続できないようにします。[Inherit] チェックボックスがオフの場合、デフォルト値は [None] です。

ステップ 8 [Store Password on Client System] 設定をグループから継承するかどうかを指定します。

[Inherit] チェックボックスをオフにすると、[Yes] および [No] のオプション ボタンが有効になります。[Yes] をクリックすると、ログインパスワードがクライアントシステムに保存されず (セキュリティが低下するおそれのあるオプションです)。接続ごとにユーザーにパスワードの入力を求めるようにするには、[No] をクリックします (デフォルト)。セキュリティを最大限に確保するためにも、パスワードの保存を許可しないことを推奨します。

ステップ 9 [Connection Settings] を設定します。

- a) このユーザーに適用するアクセス時間ポリシーを指定する、そのユーザーの新しいアクセス時間ポリシーを作成する、または [Inherit] チェックボックスをオンのままにします。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [Unrestricted] です。

[Manage] をクリックして、[Add Time Range] ダイアログボックスを開きます。このダイアログボックスでアクセス時間の新規セットを指定できます。

- b) ユーザーによる同時ログイン数を指定します。Simultaneous Logins パラメータは、このユーザーに指定できる最大同時ログイン数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザー アクセスを禁止します。

(注) 最大値を設定して制限しておかない同時に多数の接続が許可されるため、セキュリティとパフォーマンスの低下を招くおそれがあります。

- c) VPN 接続の [Maximum Connect Time] を分単位で指定します。ここで指定した時間が経過すると、システムは接続を終了します。

[Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザー接続時間を分単位で指定します。最小値は 1 分、最大値は 35791394 分 (4000 年超) です。制限なしの接続時間を許可するには、[Unlimited] をオンにします (デフォルト)。

- d) VPN 接続の [Idle Timeout] を分単位で指定します。この期間に接続で通信アクティビティがない場合、接続は終了します。

[Inherit] チェックボックスがオフになっている場合、このパラメータでアイドルタイムアウトを分単位で指定します。最小時間は 1 分、最大時間は 10080 分であり、デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。

ステップ 10 [Timeout Alerts] を設定します。

- a) [Maximum Connection Time Alert Interval] を指定します。

[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、最大接続アラート間隔は 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ~ 30 分のセッションアラート間隔を指定します。

- b) [Idle Alert Interval] を指定します。

[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、アイドルアラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ~ 30 分のセッションアラート間隔を指定します。

ステップ 11 このユーザーに対して専用の IPv4 アドレスを設定する場合は、[Dedicated IPv4 Address (Optional)] 領域で、IPv4 アドレスとサブネット マスクを入力します。

ステップ 12 このユーザーに専用の IPv6 アドレスを設定するには、[Dedicated IPv6 Address (Optional)] 領域に IPv6 プレフィックスを含む IPv6 アドレスを入力します。IPv6 プレフィックスは、IPv6 アドレスが常駐するサブネットを示します。

- ステップ 13** 特定のAnyConnect クライアントを設定します。これは、左側ペインでこれらのオプションをクリックすることにより行います。各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。
- ステップ 14** 実行コンフィギュレーションに変更を適用するには、[OK] をクリックします。

接続プロファイル

接続プロファイル（トンネルグループとも呼ばれる）では、VPN 接続の接続属性を設定します。これらの属性は、AnyConnect VPN クライアントの AnyConnect VPN モジュール、クライアントレス SSL VPN 接続、および IKEv1 と IKEv2 のサードパーティ VPN クライアントに適用されます。

AnyConnect クライアント 接続プロファイル、メインペイン

AnyConnect クライアント 接続プロファイルのメインペインでは、インターフェイス上のクライアントアクセスを有効にして、接続プロファイルを追加、編集、および削除できます。ログイン時にユーザーが特定の接続を選択できるようにするかどうかも指定できます。

- [Access Interfaces] : アクセスをイネーブルにするインターフェイスをテーブルから選択できます。このテーブルのフィールドには、インターフェイス名やチェックボックスが表示され、アクセスを許可するかどうかを指定します。

- [インターフェイス (Interface)] テーブルの AnyConnect クライアント接続に設定するインターフェイスの行で、インターフェイスでイネーブルにするプロトコルをオンにします。SSL アクセス、IPSec アクセス、またはその両方を許可できます。

SSL をオンにすると、DTLS (Datagram Transport Layer Security) がデフォルトでイネーブルになります。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。

IPsec (IKEv2) アクセスをオンにすると、クライアント サービスがデフォルトでイネーブルになります。クライアントサービスには、ソフトウェア更新、クライアントプロファイル、GUI のローカリゼーション (翻訳) とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張 AnyConnect クライアント機能が含まれています。クライアントサービスを無効にしても、AnyConnect クライアントでは IKEv2 との基本的な IPsec 接続が確立されます。

- [Device Certificate] : RSA キーまたは ECDSA キーの認証の証明書を指定できます。[デバイス証明書の指定 \(55 ページ\)](#) を参照してください。
- [Port Setting] : HTTPS および DTLS (RA クライアントのみ) 接続のポート番号を設定します。[接続プロファイル、ポート設定 \(56 ページ\)](#) を参照してください。
- [Bypass interface access lists for inbound VPN sessions] : [Enable inbound VPN sessions to bypass interface ACLs] がデフォルトでオンになっています。セキュリティアプライア

ンスが、すべての VPN トラフィックのインターフェイス ACL の通過を許可します。たとえば、外部インターフェイス ACL が復号化されたトラフィックの通過を許可しない場合でも、セキュリティ アプライアンスはリモートプライベート ネットワークを信頼し、復号化されたパケットの通過を許可します。このデフォルトの動作を変更できます。インターフェイス ACL に VPN 保護対象トラフィックの検査を行わせるためには、このチェックボックスをオフにします。

- Login Page Setting

- ユーザーはそのエイリアスで識別される接続プロファイルをログインページで選択できます。このチェックボックスをオンにしない場合、デフォルト接続プロファイルは DefaultWebVPNGroup です。
- [Shutdown portal login page.] : ログインがディセーブルの場合に Web ページを表示します。

- [Connection Profiles] : 接続（トンネルグループ）のプロトコル固有属性を設定します。

- [Add/Edit] : 接続プロファイル（トンネルグループ）を追加または編集します。
- [Name] : 接続プロファイルの名前。
- [Aliases] : 接続プロファイルの別名。
- [SSL VPN Client Protocol] : SSL VPN クライアントにアクセス権を与えるかどうかを指定します。
- [Group Policy] : この接続プロファイルのデフォルトグループポリシーを表示します。
- [Allow user to choose connection, identified by alias in the table above, at login page] : [Login] ページでの接続プロファイル（トンネルグループ）エイリアスの表示をイネーブルにする場合はオンにします。

- [Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.] : このオプションでは、接続プロファイルの選択プロセス時にグループ URL および証明書の値の相対的プリファレンスを指定します。ASA で、推奨される値と一致する値が見つからない場合は、別の値に一致する接続プロファイルが選択されます。VPN エンドポイントで指定したグループ URL を、同じグループ URL を指定する接続プロファイルと照合するために、多数の古い ASA ソフトウェア リリースで使用されるプリファレンスを利用する場合にのみ、このオプションをオンにします。このオプションは、デフォルトではオフになっています。オフにした場合、ASA は接続プロファイルで指定した証明書フィールド値を、エンドポイントで使用する証明書のフィールド値と照合して、接続プロファイルを割り当てます。

デバイス証明書の指定

[Specify Device Certificate] ペインを使用すると、接続を試みたときに、クライアントに対して ASA を識別する証明書を指定できます。この画面は、AnyConnect クライアント 接続プロフ

イルおよびクライアントレス接続プロファイル用です。Always-on IPsec/IKEv2 などの特定の AnyConnect クライアント機能では、有効で信頼できるデバイスの証明書を ASA で利用できる必要があります。

ASA リリース 9.4.1 以降では、ECDSA 証明書を（AnyConnect クライアントとクライアントレス SSL の両方からの）SSL 接続に使用できます。このリリース以前は、AnyConnect クライアント IPsec 接続用の ECDSA 証明書だけがサポートされ、設定されました。

手順

ステップ 1 (VPN 接続のみ) [Certificate with RSA Key] 領域で、次のいずれかのタスクを実行します。

- 1つの証明書を選択して、両方のプロトコルを使用してクライアントを認証する場合、[Use the same device certificate for SSL and IPsec IKEv2] チェックボックスをオンのままにします。リストボックスで使用できる証明書を選択したり、[Manage] をクリックして、使用する ID 証明書を作成したりできます。
- [Use the same device certificate for SSL and IPsec IKEv2] チェックボックスをオフにして、SSL 接続または IPsec 接続の別個の証明書を指定します。

ステップ 2 [Device Certificate] リストボックスから証明書を選択します。

必要な証明書が表示されない場合は、[Manage] ボタンをクリックして、ASA の ID 証明書を管理します。

ステップ 3 (VPN 接続のみ) [ECDSA key] フィールドの [Certificate] で、リストボックスから ECDSA の証明書を選択するか、[Manage] をクリックして、ECDSA の ID 証明書を作成します。

ステップ 4 [OK] をクリックします。

接続プロファイル、ポート設定

ASDM の接続プロファイルペインで SSL および DTLS 接続（リモートアクセスのみ）のポート番号を設定します。

[設定 (Configuration)]>[リモートアクセスVPN (Remote Access VPN)]>[ネットワーク (クライアント) アクセス (Network (Client) Access)]>[AnyConnect クライアント接続プロファイル (Connection Profiles)]

フィールド

- [HTTPS Port] : HTTPS (ブラウザベース) SSL 接続用にイネーブルにするポート。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。
- [DTLS Port] : DTLS 接続用にイネーブルにする UDP ポート。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。

AnyConnect クライアント 接続プロファイル、基本属性

Cisco Secure Client 接続の AnyConnect VPN モジュールの基本属性を設定するには、[AnyConnect クライアント接続プロファイル (Connection Profiles)] セクションで [追加 (Add)] または [編集 (Edit)] を選択します。[AnyConnect クライアント接続プロファイルの追加/編集 (Add/Edit Connection Profile)] > [基本 (Basic)] ダイアログボックスが開きます。

- [Name] : [Add] の場合、追加する接続プロファイルの名前を指定します。[Edit] の場合、このフィールドは編集できません。
- [Aliases] : (任意) この接続の代替名を 1 つ以上入力します。名前は、スペースまたは句読点で区切ることができます。
- [Authentication] : 認証の方法を、次の中から 1 つ選択し、認証処理で使用する AAA サーバーグループを指定します。
 - [Method] : 複数証明書認証のためのプロトコル交換を定義し、両方のセッションタイプでこれを利用するために認証プロトコルが拡張されています。AnyConnect クライアント SSL クライアントプロトコルと IKEv2 クライアントプロトコルを使用して、セッションごとに複数の認証を検証できます。使用する認証タイプを、AAA、AAA と証明書、証明書のみ、SAML、複数証明書および AAA、複数の証明書、SAML と証明書、または SAML と複数証明書から選択します。選択に応じて、接続するために証明書を提供する必要がある場合があります。
 - [AAA Server Group] : ドロップダウンリストから AAA サーバーグループを選択します。デフォルトの設定は LOCAL です。その場合、ASA が認証を処理するように指定されます。選択する前に、[Manage] をクリックして、このダイアログボックスの上に別のダイアログボックスを開き、AAA サーバーグループの ASA コンフィギュレーションを表示したり変更することができます。
 - LOCAL 以外のグループを選択すると、[Use LOCAL if Server Group Fails] チェックボックスが選択できるようになります。
 - [Use LOCAL if Server Group fails] : Authentication Server Group 属性によって指定されたグループに障害が発生したときに、LOCAL データベースをイネーブルにする場合はオンにします。
- [SAML ID プロバイダー (SAML Identity Provider)] : シングルサインオン (SSO) 認証用の SAML IdP サーバーを選択します。
 - [SAMLサーバー (SAML Server)] : AnyConnect クライアント シングルサインオン認証用にドロップダウンから SAML サーバーを選択するか、[管理 (Manage)] をクリックして SSO サーバーを追加し、次のパラメータを設定します。
 - [IDP エンティティ ID (IDP Entity ID)] : SAML Idp のエンティティ ID。
 - [Sign In URL] : IdP にサインインするための URL。url value は 4 ~ 500 文字の範囲で指定します。

- [Sign Out URL] (オプション) : IdP からサインインするときのリダイレクト先 URL。url value は 4 ~ 500 文字の範囲で指定します。
- [Base URL] (オプション) : エンドユーザーを ASA にリダイレクトするために、サードパーティ製 IdP に提供されます。

base-url が設定されている場合、その URL は **show saml metadata** の AssertionConsumerService と SingleLogoutService 属性のベース URL として使用されます。

base-url が設定されていない場合、URL は ASA のホスト名とドメイン名から決定されます。たとえば、ホスト名が ssl-vpn、ドメイン名が cisco.com の場合は、https://ssl-vpn.cisco.com が使用されます。

base-url もホスト名/ドメイン名も設定されていない場合は、**show saml metadata** を入力するとエラーが発生します。

- [Identity Provider Certificate] : ASA が SAML アサーションを検証するための IdP 証明書を含むトラストポイントを指定します。すでに設定されているトラストポイントを選択します。
- [Service Provider Certificate] (オプション) : IdP が ASA (SP) の署名や暗号化 SAML アサーションを検証するための ASA (SP) 証明書含むトラストポイントを指定します。すでに設定されているトラストポイントを選択します。
- [Request Signature] : ドロップダウンを使用して、SAML IdP サーバーに対して希望する署名方法を選択します。rsa-sha1、rsa-sha256、rsa-sha384、rsa-sha512 から選択できます。
- [要求タイムアウト (Request Timeout)] : (オプション) SAML 要求のタイムアウト (秒)。範囲は 1 ~ 7200 です。
指定した場合、NotBefore と timeout-in-seconds の合計が NotOnOrAfter よりも早い場合は、この設定が NotOnOrAfter に優先します。
指定しない場合は、セッションの NotBefore と NotOnOrAfter が有効期間の確認に使用されます。
- [内部ネットワークでアクセス可能な場合のみ IDP を有効化 (Enable IDP only accessible on internal network)] : 内部ネットワークでアクセス可能な場合にのみ IDP を有効にするには、このチェックボックスをオンにします。
- [ログイン時に IDP 再認証を要求 (Request IDP reauthentication at login)] : ログイン時の IDP 再認証を有効にするには、このチェックボックスをオンにします。
- [クロックスキュー (Clock-skew)] : NotBefore アサーションと NotOnOrAfter SAML アサーションを許容するクロックスキュー。デフォルトでは、クロックスキューは無効にする必要があります。デフォルト値は 1 秒で、範囲は 1 ~ 180 秒です。

- [SAML IDP TrustPoint] : シングルサインオン (SSO) 認証用の SAML IdP TrustPoint を選択します。
 - [IDP TrustPoint] : ASA が SAML アサーションを検証するための IdP 証明書を含む SAML IdP トラストポイントを選択します。
- [SAMLログインエクスペリエンス (SAML Login Experience)] : シングルサインオン (SSO) 認証用の SAML IdP TrustPoint を選択します。
 - [VPNクライアント組み込みブラウザ (VPN Client Embedded Browser)] : VPN クライアントは Web 認証に組み込みブラウザを使用するため、認証は VPN 接続にのみ適用されます。
 - [デフォルトOSブラウザ (Default OS Browser)] : VPN クライアントは、Web 認証にシステムのデフォルトブラウザを使用します。このオプションは、シングルサインオン (SSO) と、組み込みブラウザでは実行できない Web 認証方式 (生体認証など) のサポートを有効にします。

SSO 認証にデフォルトの OS ブラウザを選択する場合は、デフォルトのブラウザを使用するように AnyConnect クライアントの外部ブラウザパッケージを設定する必要があります。 [AnyConnect クライアント外部ブラウザ SAML パッケージ \(98 ページ\)](#) を参照してください。
- [SAMLユーザー名の一致 (SAML UserName Match)] : 証明書のユーザー名を SAML ユーザー名に一致させる場合に選択します。
- [Client Address Assignment] : 使用する DHCP サーバー、クライアントアドレスプール、クライアント IPv6 アドレスプールを選択します。
- [Client Address Assignment] : 使用する DHCP サーバー、クライアントアドレスプール、クライアント IPv6 アドレスプールを選択します。
 - [DHCP Servers] : 使用する DHCP サーバーの名前または IP アドレスを入力します。
 - [Client Address Pools] : クライアントアドレス割り当てで使用する、選択可能な設定済みの IPv4 アドレスプールの名前を入力します。選択する前に、[Select] をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、アドレスプールを表示したり、変更を加えたりすることができます。IPv4 アドレスプールを追加または編集する方法の詳細については [を参照してください](#)。
 - [Client IPv6 Address Pools] : クライアントアドレス割り当てで使用する、選択可能な設定済みの IPv6 アドレスプールの名前を入力します。選択する前に、[Select] をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、アドレスプールを表示したり、変更を加えたりすることができます。IPv6 アドレスプールを追加または編集する方法の詳細については [を参照してください](#)。
-
- [Default Group Policy] : 使用するグループポリシーを選択します。

- [Group Policy] : この接続のデフォルトグループポリシーとして割り当てる VPN グループポリシーを選択します。VPN グループポリシーは、ユーザー指向属性値のペアの集合で、デバイスで内部に、または RADIUS サーバーで外部に保存できます。デフォルト値は DfltGrpPolicy です。[Manage] をクリックして別のダイアログボックスを重ねて開き、グループポリシーコンフィギュレーションに変更を加えることができます。
- [Enable SSL VPN client protocol] : VPN 接続の SSL をイネーブルにする場合にオンにします。
- [Enable IPsec (IKEv2) client protocol] : 接続で IKEv2 を使用する IPsec をイネーブルにする場合にオンにします。
- [DNS Servers] : ポリシーの DNS サーバーの IP アドレスを入力します (1 つまたは複数)。
- [WINS Servers] : ポリシーの WINS サーバーの IP アドレスを入力します (1 つまたは複数)。
- [Domain] : デフォルトのドメイン名を入力します。
- [Find] : 検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

接続プロファイル、詳細属性

[Advanced] メニュー項目とそのダイアログボックスでは、この接続に関する次の特性を設定できます。

- 一般属性
- クライアントアドレス指定属性
- 認証属性
- 認可属性
- アカウンティング属性
- ネームサーバー属性



(注) SSL VPN 属性および 2 次認証属性は、SSL VPN 接続プロファイルにだけ適用されます。

AnyConnect クライアント 接続プロファイル、一般属性

- [Enable Simple Certificate Enrollment (SCEP) for this Connection Profile]

- [Strip the realm from username before passing it on to the AAA server]
- [Strip the group from username before passing it on to the AAA server]
- [Group Delimiter]
- [Enable Password Management] : ユーザーへのパスワード期限切れ通知に関するパラメータを設定できます。

- [Notify user __ days prior to password expiration] : パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時に ASDM がユーザーに通知するよう指定します。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザーへの通知を開始し、以後、ユーザーがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ~ 180 日です。

- [Notify user on the day password expires] : パスワードが期限切れになる当日にユーザーに通知します。

いずれの場合でも、変更されずにパスワードが期限切れになったとき、ASA ではユーザーによるパスワードの変更が可能です。現在のパスワードの期限が切れていなければ、ユーザーはそのパスワードで引き続きログインできます。

この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

- [Translate Assigned IP Address to Public IP Address] : まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバーおよびネットワークセキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。この機能は、トンネルグループごとに 1 つのインターフェイスでイネーブルにすることができます。

- [Enable the address translation on interface] : アドレス変換を可能にし、アドレスが表示されるインターフェイスを選択することができます。outside は AnyConnect クライアントが接続するインターフェイスであり、inside は新しいトンネルグループに固有のインターフェイスです。



(注) ルーティングの問題および他の制限事項のため、この機能が必要でない場合は、この機能の使用は推奨しません。

- [Find] : 検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

接続プロファイル、クライアントアドレス指定

接続プロファイルの [Client Addressing] ペインでは、この接続プロファイルで使用するために特定のインターフェイスに IP アドレス プールを割り当てます。[Client Addressing] ペインはすべてのクライアント接続プロファイルに共通で、次の ASDM パスからアクセスできます。

- [設定 (Configuration)]>[リモートアクセスVPN (Remote Access VPN)]>[ネットワーク (クライアント) アクセス (Network (Client) Access)]>Secure ClientAnyConnect Connection Profiles)]
- [Configuration]>[Remote Access VPN]>[Network (Client) Access]>[IPsec (IKEv1) Connection Profiles]
- [Configuration]>[Remote Access VPN]>[Network (Client) Access]>[IPsec (IKEv2) Connection Profiles]

ここで設定するアドレス プールは、接続プロファイルの [Basic] ペインでも設定できます。

AnyConnect クライアント 接続プロファイルでは、IPv4 アドレスプールだけでなく IPv6 アドレスプールも割り当てることができます。

クライアントアドレス指定を設定するには、リモート アクセス クライアント接続プロファイル (AnyConnect クライアント、IKEv1 または IKEv2) を開き、[詳細設定 (Advanced)]>[クライアントアドレッシング (Client Addressing)] を選択します。

- アドレスプールのコンフィギュレーションを表示または変更するには、ダイアログボックスの [Add] または [Edit] をクリックします。[Assign Address Pools to Interface] ダイアログボックスが開きます。このダイアログボックスでは、ASA で設定されたインターフェイスに IP アドレス プールを割り当てることができます。[Select] をクリックします。このダイアログボックスを使用して、アドレスプールのコンフィギュレーションを表示します。アドレスプールのコンフィギュレーションを変更するには、次の手順を実行します。

- ASA にアドレス プールを追加するには、[Add] をクリックします。[Add IP Pool] ダイアログボックスが開きます。
- ASA のアドレスプールのコンフィギュレーションを変更するには、[Edit] をクリックします。プール内のアドレスが使用されていない場合には、[Edit IP Pool] ダイアログボックスが開きます。

使用中の場合はアドレス プールを変更できません。[Edit] をクリックしたときにアドレス プールが使用中であった場合、ASDM は、エラー メッセージとともに、プール内のそのアドレスを使用している接続名およびユーザー名の一覧を表示します。

- ASA 上のアドレスプールの削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

使用中の場合はアドレス プールを削除できません。[Delete] をクリックしたときにアドレス プールが使用中であった場合、ASDM は、エラー メッセージとともに、プール内のそのアドレスを使用している接続名の一覧を表示します。

- アドレスプールをインターフェイスに割り当てるには、[Add] をクリックします。[Assign Address Pools to Interface] ダイアログボックスが開きます。アドレスプールを割り当てるインターフェイスを選択します。[Address Pools] フィールドの横にある [Select] をクリックします。[Select Address Pools] ダイアログボックスが開きます。インターフェイスに割り当てる個々の未割り当てプールをダブルクリックするか、または個々の未割り当てプールを選択して [Assign] をクリックします。隣のフィールドにプール割り当ての一覧が表示されます。[OK] をクリックして、これらのアドレスプールの名前を [Address Pools] フィールドに取り込み、もう一度 [OK] をクリックして割り当てのコンフィギュレーションを完了します。
- インターフェイスに割り当てられているアドレスプールを変更するには、そのインターフェイスをダブルクリックするか、インターフェイスを選択して [Edit] をクリックします。[Assign Address Pools to Interface] ダイアログボックスが開きます。アドレスプールを削除するには、各プール名をダブルクリックし、キーボードの [Delete] キーを押します。インターフェイスにその他のフィールドを割り当てている場合は、[Address Pools] フィールドの横にある [Select] をクリックします。[Select Address Pools] ダイアログボックスが開きます。[Assign] フィールドには、インターフェイスに割り当てられているアドレスプール名が表示されます。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。[OK] をクリックして、これらのアドレスプールの名前で [Address Pools] フィールドを確認し、もう一度 [OK] をクリックして割り当てのコンフィギュレーションを完了します。
- エントリを削除するには、そのエントリを選択して [Delete] をクリックします。

関連トピック

[接続プロファイル、クライアントアドレス指定、追加または編集](#) (63 ページ)

[接続プロファイル、アドレスプール](#) (64 ページ)

[接続プロファイル、詳細、IP プールの追加または編集](#) (64 ページ)

接続プロファイル、クライアントアドレス指定、追加または編集

接続プロファイルにアドレスプールを割り当てるには、[Advanced]>[Client Addressing] を選択し、[Add] または [Edit] を選択します。

- [Interface] : アドレスプールの割り当て先インターフェイスを選択します。デフォルトは DMZ です。
- [Address Pools] : 指定したインターフェイスに割り当てるアドレスプールを指定します。
- [Select] : [Select Address Pools] ダイアログボックスが開きます。このダイアログボックスでは、このインターフェイスに割り当てるアドレスプールを1つ以上選択できます。選択内容は、[Assign Address Pools to Interface] ダイアログボックスの [Address Pools] フィールドに表示されます。

接続プロファイル、アドレス プール

[Connection Profile] > [Advanced] の [Select Address Pools] ダイアログボックスに、クライアントアドレス割り当てに使用可能なアドレスプールのプール名、開始アドレスと終了アドレス、およびサブネットマスクが表示されます。そのリストを使って接続プロファイルを追加、編集、または削除できます。

- [Add] : [Add IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、新しい IP アドレス プールを設定できます。
- [Edit] : [Edit IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、選択した IP アドレス プールを変更できます。
- [Delete] : 選択したアドレス プールを削除します。確認されず、やり直しもできません。
- [Assign] : インターフェイスに割り当てられているアドレス プール名を表示します。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。

接続プロファイル、詳細、IP プールの追加または編集

[Connection Profile] > [Advanced] の [Add or Edit IP Pool] ダイアログボックスを使用すれば、クライアントアドレス割り当て用の IP アドレスの範囲を指定または変更できます。

- [Name] : IP アドレス プールに割り当てられている名前を指定します。
- [Starting IP Address] : プールの最初の IP アドレスを指定します。
- [Ending IP Address] : プールの最後の IP アドレスを指定します。
- [Subnet Mask] : プール内のアドレスに適用するサブネット マスクを選択します。

AnyConnect クライアント接続プロファイル、認証属性

[Connection Profile] > [Advanced] > [Authentication] タブで、次のフィールドを設定できます。

- [Interface-specific Authentication Server Groups] : 指定のインターフェイスに対する認証サーバー グループの割り当てを管理します。
 - [Add or Edit] : [Assign Authentication Server Group to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバーグループを指定するとともに、選択したサーバーグループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。
 - [Delete] : 選択したサーバーグループをテーブルから削除します。確認されず、やり直しもできません。

- [Username Mapping from Certificate] : ユーザー名を抽出する方法およびデジタル証明書のフィールドを指定できます。



(注) この機能はマルチ コンテキスト モードではサポートされません。

- [Pre-fill Username from Certificate] : 指定した証明書のフィールドからユーザー名を抽出し、このパネルの後に続くオプションに従って、ユーザー名/パスワード認証および認可に使用します。
- [Hide username from end user] : 抽出したユーザー名はエンドユーザーに表示されません。
- [Use script to choose username] : デジタル証明書からユーザー名を選択する場合に使用するスクリプト名を指定します。デフォルトは [None] です。
- [Add or Edit] : [Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザー名のマッピングに使用するスクリプトを定義できます。
- [Delete] : 選択したスクリプトを削除します。確認されず、やり直しもできません。
- [Use the entire DN as the username] : 証明書の [Distinguished Name] フィールド全体をユーザー名として使用する場合に指定します。
- [Specify the certificate fields to be used as the username] : ユーザー名に結合する 1 つ以上のフィールドを指定します。

プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country (国名) : 2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name (一般名) : 人、システム、その他のエンティティの前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address (電子メール アドレス)。
GENQ	Generational Qualifier (世代修飾子)。
GN	Given Name (名)。
I	Initials (イニシャル)。
L	Locality (地名) : 組織が置かれている市または町。
N	名前

属性	定義
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザー ID）。
UPN	User Principal Name（ユーザープリンシパル名）。

- [Primary Field]：ユーザー名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field]は無視されます。
- [Secondary Field]：[Primary Field]が指定されていない場合、使用するフィールドを選択します。
- [Certificate Mapping for Multi-Certificate Authentication]：プライマリ認証に使用する証明書の割り当てを管理します。
 - [First Certificate]：マシンが発行した証明書をプライマリ認証に使用する場合は、このオプションをクリックします。
 - [Second Certificate]：クライアントから発行されたユーザー証明書をプライマリ認証に使用する場合は、このオプションをクリックします。
- [Find]：検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

接続プロファイル、2次認証属性

[Connection Profile] > [Advanced] の下の [Secondary Authentication] を使用すれば、二重認証としても知られる 2 次認証を設定することができます。2 次認証が有効になっている場合は、エンドユーザーがログオンするときに有効な認証クレデンシャルを 2 セット入力する必要があります。証明書のユーザー名の事前入力と 2 次認証を組み合わせることで使用できます。このダイアログボックスのフィールドは、1 次認証で設定するフィールドと似ていますが、これらのフィールドは 2 次認証にだけ関連します。

二重認証がイネーブルになっている場合、これらの属性はユーザー名として使用する1つ以上のフィールドを証明書から選択します。証明書属性からセカンダリユーザー名を設定すると、セキュリティアプライアンスは、指定された証明書フィールドを、2次ユーザー名/パスワード認証処理に2つ目のユーザー名を使用するよう強制されます。



(注) 証明書のセカンダリユーザー名とともに2次認証サーバーグループも指定する場合でも、認証処理にはプライマリユーザー名だけが使用されます。

- **[Secondary Authorization Server Group]** : セカンダリクレデンシャルを抽出する認証サーバーグループを指定します。
 - **[Server Group]** : セカンダリサーバーAAAグループとして使用する認証サーバーグループを選択します。デフォルトはnoneです。SDIサーバーグループはセカンダリサーバーグループにできません。
 - **[Manage]** : **[Configure AAA Server Group]** ダイアログボックスが開きます。
 - **[Use LOCAL if Server Group fails]** : 指定したサーバーグループに障害が発生した場合のLOCALデータベースへのフォールバックを指定します。
 - **[Use primary username]** : ログインダイアログがユーザー名を1つだけ要求するよう指定します。
 - **[Attributes Server]** : プライマリ属性サーバーかセカンダリ属性サーバーかを選択します。



(注) この接続プロファイルにも認証サーバーを指定すると、その認証サーバーの設定が優先されます。ASAはセカンダリ認証サーバーを無視します。

- **[Session Username Server]** : プライマリセッションユーザー名サーバーかセカンダリセッションユーザー名サーバーかを指定します。
- **[Interface-Specific Authorization Server Groups]** : 指定のインターフェイスに対する認可サーバーグループの割り当てを管理します。
 - **[Add or Edit]** : **[Assign Authentication Server Group to Interface]** ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバーグループを指定するとともに、選択したサーバーグループで障害が発生した場合にLOCALデータベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの**[Manage]** ボタンをクリックすると、**[Configure AAA Server Groups]** ダイアログボックスが開きます。**[Interface/Server Group]** テーブルに選択内容が表示されます。
 - **[Delete]** : 選択したサーバーグループをテーブルから削除します。確認されず、やり直しもできません。

- [Username Mapping from Certificate] : ユーザー名を抽出するデジタル証明書のフィールドを指定できます。
- [Pre-fill Username from Certificate] : このパネルで指定されている最初のフィールドおよび2番目のフィールドから、2次認証に使用される名前を抽出する場合にオンにします。この属性をオンにする前に、AAA および証明書の認証方式を設定する必要があります。これを行うには、同じウィンドウの [Basic] パネルに戻り、[Method] の横の [Both] をオンにします。
- [Hide username from end user] : 2次認証に使用されるユーザー名を VPN ユーザーに非表示にする場合にオンにします。
- [Fallback when a certificate is unavailable] : この属性は、[Hide username from end user] がオンの場合にのみ使用可能です。証明書が使用不可な場合は、HostScan（現在は Secure Firewall ポスチャと呼ばれています） データを使用して、2次認証のユーザー名を事前入力します。
- [Password] : 2次認証に使用されるパスワードの取得方式として次のいずれかを選択します。
 - [Prompt] : ユーザーにパスワードを入力するようプロンプトを表示します。
 - [Use Primary] : すべての2次認証に1次認証のパスワードを再利用します。
 - [Use] : すべての2次認証の共通セカンダリ パスワードを入力します。
- [Specify the certificate fields to be used as the username] : ユーザー名として一致する1つ以上のフィールドを指定します。セカンダリ ユーザー名/パスワード認証または認可に証明書のユーザー名事前入力機能でこのユーザー名を使用するには、ユーザー名事前入力およびセカンダリ ユーザー名事前入力も設定する必要があります。
 - [Primary Field] : ユーザー名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field] は無視されます。
 - [Secondary Field] : [Primary Field] が指定されていない場合、使用するフィールドを選択します。

最初のフィールドおよび2番目のフィールドの属性には、次のオプションがあります。

属性	定義
C	Country（国名） : 2文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名） : 人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メールアドレス）。

属性	定義
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザー ID）。
UPN	User Principal Name（ユーザープリンシパル名）。

- [Use the entire DN as the username]：完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得します。
- [Use script to select username]：デジタル証明書からユーザー名を抽出するスクリプトを指定します。デフォルトは [None] です。
 - [Add or Edit]：[Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザー名のマッピングに使用するスクリプトを定義できます。
 - [Delete]：選択したスクリプトを削除します。確認されず、やり直しもできません。
- [Certificate Mapping for Multi-Certificate Authentication]：セカンダリ認証に使用する証明書の割り当てを管理します。
 - [First Certificate]：マシンが発行した証明書をセカンダリ認証に使用する場合は、このオプションをクリックします。
 - [Second Certificate]：クライアントから発行されたユーザー証明書をセカンダリ認証に使用する場合は、このオプションをクリックします。

AnyConnect クライアント 接続プロファイル、認可属性

AnyConnect クライアント 接続プロファイルの [認証 (Authorization)] ダイアログボックスを使用すれば、インターフェイス固有の認可サーバーグループを表示、追加、編集、または削除することができます。このダイアログボックスのテーブルの各行には、インターフェイス固有サーバーグループのステータスが表示されます。表示されるのは、インターフェイス名、それに関連付けられたサーバー グループ、および選択したサーバー グループで障害が発生したときにローカル データベースへのフォールバックがイネーブルになっているかどうかです。

このペインのフィールドは、AnyConnect クライアント、IKEv1、IKEv2、およびクライアントレス SSL 接続プロファイルで共通です。

- [Authorization Server Group] : 認可パラメータを記述する認可サーバー グループを指定します。
 - [Server Group] : 使用する認可サーバー グループを選択します。デフォルトは none です。
 - [Manage] : [Configure AAA Server Group] ダイアログボックスが開きます。
 - [Users must exist in the authorization database to connect] : ユーザーがこの基準を満たす必要がある場合は、このチェックボックスをオンにします。
- [Interface-specific Authorization Server Groups] : 指定のインターフェイスに対する認可サーバー グループの割り当てを管理します。
 - [Add or Edit] : [Assign Authentication Server Group to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバーグループを指定するとともに、選択したサーバーグループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。
 - [Delete] : 選択したサーバー グループをテーブルから削除します。確認されず、やり直しもできません。
- [Username Mapping from Certificate] : ユーザー名を抽出するデジタル証明書のフィールドを指定できます。
 - [Use script to select username] : デジタル証明書からユーザー名を選択する場合に使用するスクリプト名を指定します。デフォルトは [None] です。証明書フィールドからユーザー名を選択するスクリプトを作成する方法については、を参照してください。
 - [Add or Edit] : [Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザー名のマッピングに使用するスクリプトを定義できます。
 - [Delete] : 選択したスクリプトを削除します。確認されず、やり直しもできません。
 - [Use the entire DN as the username] : 証明書の [Distinguished Name] フィールド全体をユーザー名として使用する場合に指定します。

- [Specify the certificate fields to be used as the username] : ユーザー名に結合する 1 つ以上のフィールドを指定します。
- [Primary Field] : ユーザー名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field] は無視されます。
- [Secondary Field] : [Primary Field] が指定されていない場合、使用するフィールドを選択します。
- [Find] : 検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

AnyConnect クライアント 接続プロファイル、認可、ユーザー名を選択するためのスクリプトの内容の追加

AnyConnect クライアントの [認証 (Authorization)] ペインで [ユーザー名選択にスクリプトを使用 (use a script to select username)] を選択し、[追加 (Add)] または [編集 (Edit)] ボタンをクリックすると、次のフィールドが表示されます。

スクリプトでは、他のマッピングオプションでは表示されない認可用の証明書フィールドを使用できます。



(注) スクリプトを使用した証明書からのユーザー名事前入力でクライアント証明書のユーザー名が見つからない場合、AnyConnect クライアント およびクライアントレス WebVPN に「不明 (Unknown) 」と表示されます。

- [Script Name] : スクリプトの名前を指定します。認証および認可のスクリプト名は同じでなければなりません。ここでスクリプトを定義し、CLI は、この機能を実行するために同じスクリプトを使用します。
- [Select script parameters] : スクリプトの属性および内容を指定します。
- [Value for Username] : ユーザー名として使用する一般的な DN 属性のドロップダウン リスト (Subject DN) から属性を選択します。
- [No Filtering] : 指定した DN 名全体を使用するよう指定します。
- [Filter by substring] : 開始インデックス (一致する最初の文字の文字列内の位置) および終了インデックス (検索する文字列数) を指定します。このオプションを選択する場合、開始インデックスは、空白にはできません。終了インデックスを空白にするとデフォルトは -1 となり、文字列全体が一致するかどうか検索されます。

たとえば、ホスト/ユーザーの値を含む DN 属性の Common Name (CN) を選択したとします。次の表に、さまざまな戻り値を実現する部分文字列を使用してこの値をフィルタする方法を示します。戻り値は、ユーザー名として実際に事前入力される値です。

表 2: 部分文字列によるフィルタリング

開始インデックス	終了インデックス	戻り値
1	5	host/
6	10	user
6	-1	user

この表の3行目のようにマイナスのインデックスを使用して、文字列の最後から部分文字列の最後まで（この場合は「user」の「r」）カウントするよう指定します。

部分文字列によるフィルタリングを使用する場合、検索する部分文字列の長さがわかっていることが必要です。次の例では、正規表現照合または Lua 形式のカスタム スクリプトを使用します。

- 例 1: [Regular Expression Matching]: [Regular Expression] フィールドに検索に適用する正規表現を入力します。一般的な正規表現の演算子が適用されます。「Email Address (EA)」DN 値の @ 記号までのすべての文字列をフィルタリングするために正規表現を使用するとします。`^[^@]*` がこれを実行できる正規表現の 1 つです。この例では、DN 値に `user1234@example.com` が含まれている場合、正規表現の後の戻り値は `user1234` となります。
- 例 2: [Use custom script in LUA format]: 検索フィールドを解析するために、LUA プログラム言語で記述されたカスタムスクリプトを指定します。このオプションを選択すると、カスタム Lua スクリプトをフィールドに入力できるようになります。スクリプトは次のようになります。

```
return cert.subject.cn..'/'..cert.subject.1
```

1つのユーザー名として使用する2つのDNフィールド、ユーザー名 (cn) および地域 (l) を結合し、2つのフィールド間にスラッシュ (/) 文字を挿入します。

次の表に Lua スクリプトで使用可能な属性名と説明を示します。



(注) Lua では、大文字と小文字が区別されます。

表 3: 属性名と説明

属性名	説明
cert.subject.c	Country
cert.subject.cn	Common Name
cert.subject.dnq	DN 修飾子
cert.subject.ea	電子メール アドレス

cert.subject.genq	世代修飾子
cert.subject.gn	名
cert.subject.i	イニシャル
cert.subject.l	地名
cert.subject.n	名前
cert.subject.o	マニュアルの構成
cert.subject.ou	組織単位
cert.subject.ser	サブジェクト シリアル番号
cert.subject.sn	姓
cert.subject.sp	州/県
cert.subject.t	Title
cert.subject.uid	ユーザー ID
cert.issuer.c	Country
cert.issuer.cn	Common Name
cert.issuer.dnq	DN 修飾子
cert.issuer.ea	電子メール アドレス
cert.issuer.genq	世代修飾子
cert.issuer.gn	名
cert.issuer.i	イニシャル
cert.issuer.l	地名
cert.issuer.n	名前
cert.issuer.o	マニュアルの構成
cert.issuer.ou	組織単位
cert.issuer.ser	発行元シリアル番号
cert.issuer.sn	姓
cert.issuer.sp	州/県
cert.issuer.t	Title

cert.issuer.uid	ユーザー ID
cert.serialnumber	証明書シリアル番号
cert.subjectaltname.upn	ユーザー プリンシパル名

トンネル グループ スクリプトをアクティブにしているときにエラーが発生し、スクリプトがアクティブにならなかった場合、管理者のコンソールにエラー メッセージが表示されます。

接続プロファイル、アカウントिंग

[Connection Profile] > [Advanced] の [Accounting] ペインでは、ASA 全体のアカウントिंग オプションを設定します。

- [Accounting Server Group] : アカウントिंगに使用するすでに定義済みのサーバー グループを選択します。
- [Manage] : AAA サーバー グループを作成できる [Configure AAA Server Groups] ダイアログボックスが開きます。

接続プロファイル、グループエイリアスとグループ URL

[Connection Profile] > [Advanced] の [GroupAlias/Group Group URL] ダイアログボックスで、リモートユーザーのログイン時に表示される内容に影響を与える属性を設定します。

接続プロファイルのタブの名前は、AnyConnect クライアントでは、[グループURL/グループエイリアス (Group URL/Group Alias)] です。

- [Login and Logout (Portal) Page Customization (Clientless SSL VPN only)] : 適用する事前設定されたカスタマイズ属性を指定することにより、ユーザー ログイン ページの外観を設定します。デフォルトは DfltCustomization です。新しいカスタマイゼーションオブジェクトを作成するには、[Manage] をクリックします。
- [Enable the display of Radius Reject-Message on the login screen] : 認証が拒否されたときにログイン ダイアログボックスに RADIUS-reject メッセージを表示するには、このチェックボックスをオンにします。
- [Enable the display of SecurID message on the login screen] : ログイン ダイアログボックスに SecurID メッセージを表示するには、このチェックボックスをオンにします。
- [Connection Aliases] : 接続エイリアスとそのステータス。ログイン時にユーザーが特定の接続 (トンネルグループ) を選択できるように接続が設定されている場合は、ユーザーのログイン ページに接続エイリアスが表示されます。エイリアスを追加または削除するには、[Add] または [Delete] ボタンをクリックします。エイリアスを編集するには、テーブルでそのエイリアスをダブルクリックし、エントリを編集します。イネーブルになっているステータスを変更するには、テーブル内のチェックボックスをオンまたはオフにします。

- [Group URLs] : グループ URL とそのステータス。ログイン時にユーザーが特定のグループを選択できるように接続が設定されている場合は、ユーザーのログインページにグループ URL が表示されます。URL を追加または削除するには、[Add] または [Delete] ボタンをクリックします。URL を編集 ([Edit]) するには、テーブル内の URL をダブルクリックしてエントリを編集します。イネーブルになっているステータスを変更するには、テーブル内のチェックボックスをオンまたはオフにします。

IKEv1 接続プロファイル

IKEv1 接続プロファイルは、L2TP/IPsec などのネイティブ VPN クライアントとサードパーティ VPN クライアントの認証ポリシーを定義します。IKEv1 接続プロファイルは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] ペインで設定します。

- [Access Interfaces] : IPsec アクセスでイネーブルにするインターフェイスを選択します。デフォルトでは、アクセス方式は何も選択されていません。
- [Connection Profiles] : 既存の IPsec 接続の設定済みパラメータを表形式で表示します。[Connections] テーブルには、接続ポリシーを決定するレコードが表示されます。1 つのレコードによって、その接続のデフォルト グループ ポリシーが識別されます。レコードにはプロトコル固有の接続パラメータが含まれています。テーブルには、次のカラムがあります。
 - [Name] : IPsec IKEv1 接続の名前または IP アドレスを指定します。
 - [IPsec Enabled] : IPsec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPsec Remote Access Connection] の [Basic] ダイアログボックスでイネーブルにします。
 - [L2TP/IPsec Enabled] : L2TP/IPsec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPsec Remote Access Connection] の [Basic] ダイアログボックスでイネーブルにします。
 - [Authentication Server Group] : 認証を提供できるサーバー グループの名前。
 - [Group Policy] : この IPsec 接続のグループ ポリシーの名前を示します。



(注) [Delete] : 選択したサーバー グループをテーブルから削除します。確認されず、やり直しもできません。

IPsec リモート アクセス接続プロファイル、[Basic] タブ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] > [Add/Edit] > [Basic] の [Add or Edit IPsec Remote Access Connection Profile Basic] ダイア

ログボックスを使用すると、L2TP-IPsec を含めて、IPsec IKEv1 VPN 接続用の共通属性を設定できます。

- [Name] : 接続プロファイルの名前。
- [IKE Peer Authentication] : IKE ピアを設定します。
 - [Pre-shared key] : 接続用の事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Identity Certificate] : ID 証明書が設定され、登録されている場合は、ID 証明書の名前を選択します。[Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、選択した証明書の詳細を追加、編集、削除、エクスポート、表示できます。
- [User Authentication] : ユーザー認証で使用するサーバーの情報を指定します。詳細な認証情報は [Advanced] セクションで設定できます。
 - [Server Group] : ユーザー認証で使用するサーバー グループを選択します。デフォルトは LOCAL です。LOCAL 以外のサーバー グループを選択すると、[Fallback] チェックボックスが選択できるようになります。サーバーグループを追加するには、[Manage] ボタンをクリックします。
 - [Fallback] : 指定したサーバー グループで障害が発生した場合に、ユーザー認証で LOCAL を使用するかどうかを指定します。
- [Client Address Assignment] : クライアント属性の割り当てに関連する属性を指定します。
 - [DHCP Servers] : 使用する DHCP サーバーの IP アドレスを指定します。最大で 10 台までのサーバーをスペースで区切って追加できます。
 - [Client Address Pools] : 事前定義済みのアドレス プールを 6 個まで指定します。アドレス プールを定義するには、[Select] ボタンをクリックします。
- [Default Group Policy] : デフォルト グループ ポリシーに関連する属性を指定します。
 - [Group Policy] : この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。このグループ ポリシーに関連付ける新しいグループ ポリシーを定義するには、[Manage] をクリックします。
 - [Enable IPsec protocol] と [Enable L2TP over IPsec protocol] : この接続で使用するプロトコルを選択します。

[Add/Edit Remote Access Connections] > [Advanced] > [General]

このダイアログボックスを使用して、AAA サーバーに渡す前にユーザー名からレルムとグループを除去するかどうかを指定し、パスワード管理パラメータを指定します。

- [Strip the realm from the username before passing it on to the AAA server] : ユーザー名を AAA サーバーに渡す前に、レルム（管理ドメイン）をユーザー名から除去する処理をイネーブ

ルまたはディセーブルにします。認証時にユーザー名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザー名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@example.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザー名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバーでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。



(注) レルムとグループの両方をユーザー名に追加できます。その場合、ASA は、AAA 機能に対してグループ用とレルム用に設定されたパラメータを使用します。このオプションの形式は、ユーザー名[@realm][<# または !>グループ] となります（例：JaneDoe@example.com#VPNGroup）。このオプションを選択した場合は、グループデリミタとして # または ! を使用する必要があります。これは、@ がレルムデリミタとしても使用されている場合、ASA が @ をグループデリミタと解釈できないからです。

Kerberos レルムは特殊事例です。Kerberos レルムの命名規則として、Kerberos レルムと関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザーが example.com ドメインに存在する場合には、Kerberos レルムを EXAMPLE.COM と表記します。

ASA には、user@grouppolicy のサポートは含まれません。L2TP/IPsec クライアントだけが、user@tunnelgroup を介したトンネルスイッチングをサポートしています。

- [Strip the group from the username before passing it on to the AAA server] : ユーザー名を AAA サーバーに渡す前に、レルム（管理ドメイン）をユーザー名から除去する処理をイネーブルまたはディセーブルにします。認証時にユーザー名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザー名に追加し、Group Lookup をイネーブルにすると、ASA は、デリミタの左側にある文字をすべてユーザー名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループデリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。ユーザー名<デリミタ>グループの形式でグループをユーザー名に追加します（例：JaneDoe@VPNGroup、JaneDoe#VPNGroup や JaneDoe!VPNGroup）。
- [Password Management] : AAA サーバーからの account-disabled インジケータの上書きに関するパラメータと、ユーザーに対するパスワード期限切れ通知に関するパラメータを設定できます。
 - [Enable notification upon password expiration to allow user to change password] : このチェックボックスをオンにすると、次の2つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザーに通知するか、またはパスワードが期限切れになる当日にユーザーに

通知するかを選択できます。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザーへの通知を開始し、以後、ユーザーがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ~ 180 日です。



- (注) この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

いずれの場合でも、変更されずにパスワードが期限切れになったとき、ASA ではユーザーによるパスワードの変更が可能です。現行のパスワードが失効していない場合、ユーザーはそのパスワードを使用してログインし続けることができます。

このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバー、LDAP サーバーなどの AAA サーバーで有効です。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

この機能では、MS-CHAPv2 を使用する必要があります。

IKEv1 クライアントアドレス指定

クライアントアドレス指定の設定はすべてのクライアント接続プロファイルに共通です。詳細については、[接続プロファイル](#)、[クライアントアドレス指定 \(62 ページ\)](#) を参照してください。

IKEv1 接続プロファイル、認証

このダイアログボックスは、IPsec on Remote Access および Site-to-Site トンネルグループの場合に表示されます。このダイアログボックスでの設定は、ASA 全体に渡ってこの接続プロファイル（トンネルグループ）に適用されます。インターフェイスごとに認証サーバーグループを設定するには、[Advanced] をクリックします。このダイアログボックスでは、次の属性を設定できます。

- [Authentication Server Group] : LOCAL グループ（デフォルト）などの利用可能な認証サーバーグループを一覧表示します。None も選択可能です。None または Local 以外を選択すると、[Use LOCAL if Server Group Fails] チェックボックスが利用できるようになります。
- [Use LOCAL if Server Group fails] : Authentication Server Group 属性によって指定されたグループで障害が発生した場合に、LOCAL データベースへのフォールバックをイネーブルまたはディセーブルにします。

[Enable Group Lookup] ボックスをオフにすると、ユーザー名のみに基づく認証を設定できます。[Enable Group Lookup] ボックスと [Strip Group] の両方をオンにすると、AAA サーバーでグループ名が付加されたユーザーのデータベースを維持しながら、同時にユーザー名のみに基づいてユーザーを認証することができます。

IKEv1 接続プロファイル、認可

認可の設定はすべてのクライアント接続プロファイルに共通です。詳細については、[AnyConnect クライアント接続プロファイル、認証属性 \(64 ページ\)](#) を参照してください。

IKEv1 接続プロファイル、アカウントティング

アカウントティングの設定はすべてのクライアント接続プロファイルに共通です。詳細については、[接続プロファイル、アカウントティング \(74 ページ\)](#) を参照してください。

IKEv1 接続プロファイル、IPsec

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edi] > [Advanced] > [IPsec]

- [Send certificate chain] : 証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [IKE Peer ID Validation] : IKE ピア ID 検証を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- [IKE Keep Alive] : ISAKMP キープアライブ モニタリングをイネーブルにして設定します。
 - [Disable Keep Alives] : ISAKMP キープアライブをイネーブルまたはディセーブルにします。
 - [Monitor Keep Alives] : ISAKMP キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
 - [Confidence Interval] : ISAKMP キープアライブの信頼間隔を指定します。これは、ASA がキープアライブモニタリングを開始するまでに、ピアがアイドル状態を継続できる秒数です。最小 10 秒、最大 300 秒です。リモートアクセス グループのデフォルトは 300 秒です。
 - [Retry Interval] : ISAKMP キープアライブのリトライ間の待機秒数を指定します。デフォルト値は 2 秒です。
 - [Head end will never initiate keepalive monitoring] : 中央サイトの ASA がキープアライブモニタリングを開始しないように指定します。

IKEv1 接続プロファイル、IPsec、IKE 認証

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edi] > [Advanced] > [IPsec] > [IKE Authentication]

- [Default Mode] : 上記の none、xauth、または hybrid からデフォルトの認証モードを選択できます。

- [Interface-Specific Mode] : 認証モードをインターフェイスごとに指定します。
 - [Add/Edit/Delete] : [Interface/Authentication Modes] テーブルに対して、選択したインターフェイスと認証モードのペアを追加/編集/削除します。
 - [Interface] : 名前付きインターフェイスを選択します。デフォルトのインターフェイスは `inside` と `outside` ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
 - [Authentication Mode] : 上記の `none`、`xauth`、または `hybrid` から認証モードを選択できます。

IKEv1 接続プロファイル、IPsec、クライアントソフトウェアの更新

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edit] > [Advanced] > [IPsec] > [Client Software Update]

[Client VPN Software Update Table] : インストールされている各クライアント VPN ソフトウェアパッケージについて、クライアントタイプ、VPNクライアントのリビジョン、およびイメージ URL を一覧表示します。クライアントタイプごとに、許可されるクライアントソフトウェアリビジョンと、必要に応じて、ソフトウェアアップグレードをダウンロードする URL または IP アドレスを指定できます。クライアントアップデートメカニズム (Client Update ダイアログボックスに詳細説明があります) は、この情報を使用して、各 VPN クライアントが適切なリビジョンレベルで実行されているかどうか、適切であれば、通知メッセージとアップデートメカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。

- [Client Type] : VPN クライアントタイプを識別します。
- [VPN Client Revisions] : 許可される VPN クライアントのリビジョンレベルを指定します。
- [Location URL] : 適切な VPN クライアントソフトウェアイメージをダウンロードできる URL または IP アドレスを指定します。ダイアログボックススペースの VPN クライアントの場合、URL は `http://` または `https://` という形式です。クライアントモードの ASA 5505 では、URL は `tftp://` 形式である必要があります。

IKEv1 接続プロファイル、PPP

この IKEv1 接続プロファイルを使用して PPP 接続で許可される認証プロトコルを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] > [Add/Edit] > [Advanced] > [PPP] を開きます。

このダイアログボックスは、IPsec IKEv1 リモートアクセス接続プロファイルにだけ適用されます。

- [CHAP] : PPP 接続で CHAP プロトコルの使用をイネーブルにします。
- [MS-CHAP-V1] : PPP 接続で MS-CHAP-V1 プロトコルの使用をイネーブルにします。

- [MS-CHAP-V2] : PPP 接続で MS-CHAP-V2 プロトコルの使用をイネーブルにします。
- [PAP] : PPP 接続で PAP プロトコルの使用をイネーブルにします。
- [EAP-PROXY] : PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。EAP は、Extensible Authentication protocol (拡張認証プロトコル) を意味します。

IKEv2 接続プロファイル

IKEv2 接続プロファイルでは、Cisco Secure Client の AnyConnect VPN モジュールに対する EAP、証明書ベース、および事前共有キー ベースの認証を定義します。ASDM の設定パネルは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles] です。

- [Access Interfaces] : IPsec アクセスでイネーブルにするインターフェイスを選択します。デフォルトでは、アクセス方式は何も選択されていません。
- [Bypass interface access lists for inbound VPN sessions] : 着信 VPN セッションのインターフェイスアクセスリストをバイパスするには、このチェックボックスをオンにします。グループポリシーおよびユーザー ポリシーのアクセス リストはすべてのトラフィックに常に適用されます。
- [Connection Profiles] : 既存の IPsec 接続の設定済みパラメータを表形式で表示します。[Connection Profiles] テーブルには、接続ポリシーを決定するレコードが表示されます。1 つのレコードによって、その接続のデフォルトグループポリシーが識別されます。レコードにはプロトコル固有の接続パラメータが含まれています。テーブルには、次のカラムがあります。
 - [Name] : IPsec 接続の名前または IP アドレスを指定します。
 - [IKEv2 Enabled] : オンになっている場合は、IKEv2 プロトコルがイネーブルになっていることを示します。
 - [Authentication Server Group] : 認証に使用するサーバー グループの名前を指定します。
 - [Group Policy] : この IPsec 接続のグループ ポリシーの名前を示します。



(注) [Delete] : 選択したサーバー グループをテーブルから削除します。確認されず、やり直しもできません。

IPsec IKEv2 接続プロファイル : [Basic] タブ

[Add or Edit IPsec Remote Access Connection Profile Basic] ダイアログボックスでは、IPsec IKEv2 接続の共通属性を設定します。

- [Name] : 接続名を特定します。
- [IKE Peer Authentication] : IKE ピアを設定します。
 - [Pre-shared key] : 接続用の事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Enable Certificate Authentication] : オンにすると、認証に証明書を使用できます。
 - [Enable peer authentication using EAP] : オンにすると、認証に EAP を使用できます。このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。
 - [Send an EAP identity request to the client] : リモートアクセス VPN クライアントに EAP 認証要求を送信できます。
- [Mobike RRC] : Mobike RRC を有効/無効にします。
 - [Enable Return Routability Check for mobike] : Mobike が有効になっている IKE/IPSEC セキュリティ アソシエーションにおけるダイナミック IP アドレスの変更をチェックする Return Routability を有効/無効にします。
- [User Authentication] : ユーザー認証で使用するサーバーの情報を指定します。詳細な認証情報は [Advanced] セクションで設定できます。
 - [Server Group] : ユーザー認証で使用するサーバー グループを選択します。デフォルトは LOCAL です。LOCAL 以外のサーバー グループを選択すると、[Fallback] チェックボックスが選択できるようになります。
 - [Manage] : [Configure AAA Server Group] ダイアログボックスが開きます。
 - [Fallback] : 指定したサーバー グループで障害が発生した場合に、ユーザー認証で LOCAL を使用するかどうかを指定します。
- [Client Address Assignment] : クライアント属性の割り当てに関連する属性を指定します。
 - [DHCP Servers] : 使用する DHCP サーバーの IP アドレスを指定します。最大で 10 台までのサーバーをスペースで区切って追加できます。
 - [Client Address Pools] : 事前定義済みのアドレスプールを 6 個まで指定します。[Select] をクリックすると、[Address Pools] ダイアログボックスが開きます。
- [Default Group Policy] : デフォルト グループ ポリシーに関連する属性を指定します。
 - [Group Policy] : この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。
 - [Manage] : [Configure Group Policies] ダイアログボックスが開きます。このダイアログボックスでは、グループ ポリシーを追加、編集、または削除できます。
 - [Client Protocols] : この接続で使用するプロトコルを選択します。デフォルトでは、IPsec と L2TP over IPsec の両方が選択されています。

- [Enable IKEv2 Protocol] : リモート アクセス接続 プロファイルで使用する IKEv2 プロトコルをイネーブルにします。これは、先ほど選択したグループ ポリシーの属性です。

IPsec リモート アクセス接続 プロファイル : [Advanced] > [IPsec] タブ

IPsec (IKEv2) 接続プロファイルの [IPsec] テーブルに次のフィールドがあります。

- [Send certificate chain] : 証明書チェーン全体の送信をイネーブルまたはディセーブルにする場合にオンにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [IKE Peer ID Validation] : IKE ピア ID の有効性をチェックしないか、必須とするか、あるいは証明書によってサポートされている場合にチェックするかをドロップダウンリストから選択します。

IPsec または SSLVPN 接続 プロファイルへの証明書のマッピング

ASA は、クライアント証明書認証による IPsec 接続要求を受信すると、設定されているポリシーに従って接続に接続プロファイルを割り当てます。そのポリシーは、設定したルールを使用でき、証明書 OU フィールド、IKE ID (ホスト名、IP アドレス、キー ID など)、ピア IP アドレス、またはデフォルト接続プロファイルを使用できます。SSL 接続の場合、ASA は設定されているルールだけを使用します。

ルールを使用する IPsec 接続または SSL 接続の場合、ASA は一致するものが見つかるまでルールに対して証明書の属性を評価します。一致するルールが見つかったら、そのルールに関連付けられた接続プロファイルを接続に割り当てます。一致するルールが見つからない場合、ASA は、デフォルトの接続プロファイル (IPsec の場合は DefaultRAGroup、SSL VPN の場合は DefaultWEBVPNGroup) を接続に割り当てます。ユーザーは、接続プロファイルがイネーブルになっていれば、ポータルページに表示されるドロップダウンリストからその接続プロファイルを選択できます。この接続プロファイルの接続を 1 回試みた場合の結果は、証明書が有効かどうか、そして接続プロファイルの認証設定によって異なります。

ポリシーに一致する証明書グループは、証明書ユーザーの権限グループを特定するために使用する方法を定義します。

[Policy] ペインで照合するポリシーを設定します。照合するルールを選択する場合は、[Rules] ペインに移動してルールを指定します。

証明書/接続プロファイル マップ、ポリシー

IPsec 接続において、ポリシーに一致する証明書グループは、証明書ユーザーの権限グループを特定するために使用する方法を定義します。これらのポリシーの設定項目は、[Configuration]

> [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] > [Policy] で設定します。

- [Use the configured rules to match a certificate to a group] : [Rules] で定義したルールを使用できます。
- [Use the certificate OU field to determine the group] : 組織ユニットフィールドを使用して、証明書に一致するグループを決定できます。この設定は、デフォルトでオンになっています。
- [Use the IKE identity to determine the group] : [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [IKE Parameters] で定義した ID を使用できます。IKE ID は、IP アドレス、キー ID により、または自動で指定されます。
- [Use the peer IP address to determine the group] : ピアの IP アドレスを使用できます。この設定は、デフォルトでオンになっています。
- [Default to Connection Profile] : どの方法にも一致しなかった場合に使用する、証明書ユーザーのデフォルトグループを選択できます。この設定は、デフォルトでオンになっています。[Default]にあるデフォルトグループをクリックして、リストをグループ化します。設定にはグループが必要です。リスト内にグループがない場合は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] でグループを定義する必要があります。

証明書/接続プロファイル マップのルール

IPsec 接続において、ポリシーに一致する証明書グループは、証明書ユーザーの権限グループを特定するために使用する方法を定義します。プロファイルマップは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] > [Rules] で作成します。

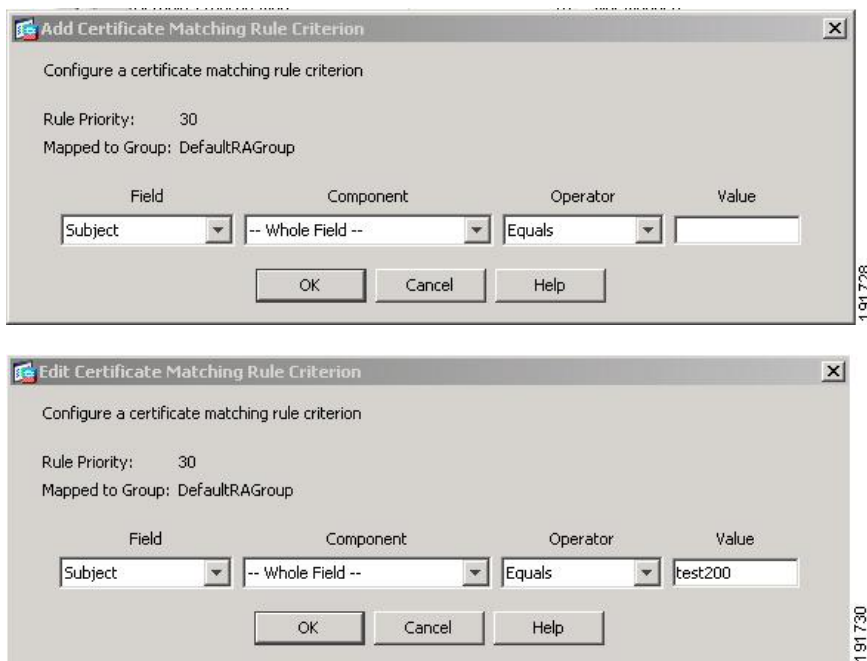
このペインには、証明書/接続プロファイルマップのリストとマッピング基準が表示されます。

証明書/接続プロファイル マップ、証明書照合ルール基準の追加

接続プロファイルをマッピングルールにマップするマッププロファイルを作成します。

- [Map] : 次のいずれかを選択します。
 - [Existing] : ルールを含めるマップの名前を選択します。
 - [New] : ルールの新しいマップ名を入力します。
- [Priority] : 10 進数を入力して、接続要求を受け取ったときに ASA がマップを評価する順序を指定します。定義されている最初のルールのデフォルトプライオリティは 10 です。ASA は各接続を評価する際に、優先順位番号が最も小さいマップから評価します。
- [Mapped to Connection Profile] : 以前は「トンネルグループ」と呼んでいた接続プロファイルを選択して、このルールにマッピングします。

次の項で説明するマップへのルール基準の割り当てを行わない場合、ASA はそのマップ エントリを無視します。



証明書照合ルール基準の追加/編集

このダイアログボックスは、接続プロファイルにマッピング可能な証明書照合ルール基準を設定するために使用します。

- [Rule Priority] : (表示専用) 接続要求を受け取ったときに ASA がマップを評価する順序。ASA は各接続を評価する際に、優先順位番号が最も小さいマップから評価します。
- [Mapped to Group] : (表示専用) ルールが割り当てられている接続プロファイル。
- [Field] : ドロップダウン リストから、評価する証明書の部分を選択します。
 - [Subject] : 証明書を使用するユーザーまたはシステム。CA のルート証明書の場合は、Subject と Issuer が同じです。
 - [Alternative Subject] : サブジェクト代替名拡張により、追加する ID を証明書のサブジェクトにバインドできます。
 - [Issuer] : 証明書を発行した CA または他のエンティティ (管轄元)。
 - [Extended Key Usage] : 一致の候補として選択できる、より高度な基準を提供するクライアント証明書の拡張。
- [Component] : ([Subject of Issuer] が選択されている場合にのみ適用されます)。ルールで使用する識別名コンポーネントを次の中から選択します。

DN フィールド	定義
Whole Field	DN 全体。
Country (C)	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠していません。
Common Name (CN)	ユーザー、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier (DNQ)	特定の DN 属性。
E-mail Address (EA)	証明書を所有するユーザー、システム、またはエンティティの電子メールアドレス。
Generational Qualifier (GENQ)	Jr.、Sr.、または III などの世代修飾子。
Given Name (GN)	証明書所有者の名前（名）。
Initials (I)	証明書所有者の姓と名の最初の文字。
Locality (L)	組織が所在する市町村。
Name (N)	証明書所有者の名前。
Organization (O)	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit (OU)	組織内のサブグループ。
Serial Number (SER)	証明書のシリアル番号。
Surname (SN)	証明書所有者の姓。
State/Province (S/P)	組織が所在する州や県。
Title (T)	証明書所有者の役職（Dr. など）。
User ID (UID)	証明書所有者の ID 番号。
Unstructured Name (UNAME)	unstructuredName 属性タイプは、サブジェクトの名前を非構造化 ASCII 文字列として指定します。
IP Address (IP)	IP アドレス フィールド。

- [Operator] : ルールで使用する演算子を選択します。
 - [Equals] : 認定者名フィールドが値に完全一致する必要があります。
 - [Contains] : 認定者名フィールドに値が含まれている必要があります。

- [Does Not Equal] : 認定者名フィールドが値と一致しないようにします。
- [Does Not Contain] : 認定者名フィールドに値が含まれないようにします。
- [Value] : 255 文字までの範囲で演算子のオブジェクトを指定します。Extended Key Usage 機能の場合、ドロップダウンリストで事前定義された値のいずれかを選択するか、他の拡張の OID を入力できます。事前定義された値は次のとおりです。

選択項目	キー使用の目的	OID 文字列
clientauth	クライアント認証	1.3.6.1.5.5.7.3.2
codesigning	コード署名	1.3.6.1.5.5.7.3.3
emailprotection	安全な電子メール保護	1.3.6.1.5.5.7.3.4
ocspsigning	OCSP 署名	1.3.6.1.5.5.7.3.9
serverauth	サーバー認証	1.3.6.1.5.5.7.3.1
timestamping	タイムスタンプ	1.3.6.1.5.5.7.3.8

Site-to-Site 接続プロファイル

[Connection Profiles] ダイアログボックスには、現在設定されている Site-to-Site 接続プロファイル（トンネルグループ）の属性が表示されます。このダイアログボックスを使用すれば、接続プロファイル名を解析するとき使用するデリミタを選択したり、接続プロファイルを追加、変更、または削除したりすることもできます。

ASA では、IPv4 または IPv6 の IPsec LAN-to-LAN VPN 接続は IKEv1 または IKEv2 を使用してサポートされ、内部ネットワークと外部ネットワークは内部および外部 IP ヘッダーを使用してサポートされます。

[Site to Site Connection Profile] ペインのフィールド

- [Access Interfaces] : インターフェイスのリモートピアデバイスによってアクセスできるデバイス インターフェイスのテーブルが表示されます。
 - [Interface] : アクセスをイネーブルまたはディセーブルにするデバイス インターフェイス。
 - [Allow IKEv1 Access] : ピアデバイスによる IPsec IKEv1 アクセスをイネーブルにする場合にオンにします。
 - [Allow IKEv2 Access] : ピアデバイスによる IPsec IKEv2 アクセスをイネーブルにする場合にオンにします。

- [Connection Profiles] : プロファイルを追加、編集、または削除できる接続プロファイルのテーブルを表示します。
 - [Add] : [Add IPsec Site-to-Site connection profile] ダイアログボックスが開きます。
 - [Edit] : [Edit IPsec Site-to-Site connection profile] ダイアログボックスが開きます。
 - [Delete] : 選択した接続プロファイルを削除します。確認されず、やり直しもできません。
 - [Name] : 接続プロファイルの名前。
 - [Interface] : 接続プロファイルがイネーブルになっているインターフェイス。
 - [Local Network] : ローカル ネットワークの IP アドレスを指定します。
 - [Remote Network] : リモート ネットワークの IP アドレスを指定します。
 - [IKEv1 Enabled] : 接続プロファイルに対してイネーブルになっている IKEv1 を表示します。
 - [IKEv2 Enabled] : 接続プロファイルに対してイネーブルになっている IKEv2 を表示します。
 - [Group Policy] : 接続プロファイルのデフォルト グループ ポリシーを表示します。

Site-to-Site 接続プロファイル、追加または編集

[Add or Edit IPsec Site-to-Site Connection] ダイアログボックスでは、IPsec Site-to-Site 接続を作成または変更できます。このダイアログボックスでは、IP アドレス (IPv4 または IPv6) の指定、接続名の指定、インターフェイスの選択、IKEv1 ピアおよび IKEv2 ピアとユーザー認証パラメータの指定、保護されたネットワークの指定、および暗号化アルゴリズムの指定を行うことができます。



- (注) サイト間 VPN 接続プロファイルを作成する場合、接続プロファイルを開き、構成を変更せずにキャンセルします。[Apply] ボタンが強調表示されている場合は、変更を破棄します。

2つのピアの内部および外部ネットワークが IPv4 の場合 (内部および外部インターフェイス上のアドレスが IPv4 の場合)、ASA では、シスコまたはサードパーティのピアとの LAN-to-LAN VPN 接続がサポートされます。

IPv4 アドレッシングと IPv6 アドレッシングが混在した、またはすべて IPv6 アドレッシングを使用する LAN-to-LAN 接続については、両方のピアが ASA の場合、および両方の内部ネットワークのアドレッシング方式が一致している場合 (両方が IPv4 または両方が IPv6 の場合) は、セキュリティアプライアンスで VPN トンネルがサポートされます。

具体的には、両方のピアが ASA の場合、次のトポロジがサポートされます。

- ASA の内部ネットワークが IPv4 で、外部ネットワークが IPv6（内部インターフェイス上のアドレスが IPv4 で、外部インターフェイス上のアドレスが IPv6）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv4（内部インターフェイス上のアドレスが IPv6 で、外部インターフェイス上のアドレスが IPv4）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv6（内部および外部インターフェイス上のアドレスが IPv6）

[Basic] パネルのフィールド

- [Peer IP Address] : IP アドレス (IPv4 または IPv6) を指定し、そのアドレスをスタティックにするかどうかを指定できます。
- [Connection Name] : この接続プロファイルに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。接続名が、[Peer IP Address] フィールドで指定される IP アドレスと同じになるように指定できます。
- [Interface] : この接続で使用するインターフェイスを選択します。
- [Protected Networks] : この接続で保護されているローカルおよびリモート ネットワークを選択または指定します。
 - [IP Address Type] : アドレスが IPv4 アドレスまたは IPv6 アドレスのいずれであるかを指定します。
 - [Local Network] : ローカル ネットワークの IP アドレスを指定します。
 - [...] : [Browse Local Network] ダイアログボックスが開きます。このダイアログボックスでは、ローカル ネットワークを選択できます。
 - [Remote Network] : リモート ネットワークの IP アドレスを指定します。
- [IPsec Enabling] : この接続プロファイルのグループ ポリシー、およびそのポリシーで指定したキー交換プロトコルを指定します。
 - [Group Policy Name] : この接続プロファイルに関連付けられているグループ ポリシーを指定します。
 - [Manage] : [Browse Remote Network] ダイアログボックスが開きます。このダイアログボックスでは、リモート ネットワークを選択できます。
 - [Enable IKEv1] : 指定したグループ ポリシーでキー交換プロトコル IKEv1 をイネーブルにします。
 - [Enable IKEv2] : 指定したグループ ポリシーでキー交換プロトコル IKEv2 をイネーブルにします。
- [IKEv1 Settings] タブ : IKEv1 の次の認証設定および暗号化設定を指定します。
 - [Pre-shared Key] : トンネルグループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。

- [Device Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。
 - [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
 - [IKE Policy] : IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
 - [Manage] : [Configure IKEv1 Proposals] ダイアログボックスが開きます。
 - [IPsec Proposal] : IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [IKEv2 Settings] タブ : IKEv2 の次の認証設定および暗号化設定を指定します。
- [Local Pre-shared Key] : トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Local Device Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。
 - [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
 - [Remote Peer Pre-shared Key] : トンネル グループのリモートピア事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [リモートピアポスト量子事前共有キー (Remote Peer Post Quantum Key)] : 事前共有キーの代わりに、IKEv2 用のポスト量子事前共有キー (PPK) を指定するには、このチェックボックスをオンにします。PPK は、256 ビット 64 文字の 16 進数文字列です。
PPK は事前共有キーに似ており、IKEv2 を量子コンピュータの攻撃から保護します。
 - [パスワードの表示 (Show Password)] : このチェックボックスをオンにすると、PPK キーが表示されます。
 - [リモートピアポスト量子キー ID (Remote Peer Post Quantum Key Identity)] : PPK の ID を指定します。
 - [Remote Peer Certificate Authentication] : この接続プロファイルの IKEv2 接続用の証明書認証を許可するには、[Allowed] をオンにします。
 - [Manage] : 証明書の表示や新規証明書の追加を実行できる [Manage CA Certificates] ダイアログが開きます。
 - [RSA 署名ハッシュを有効にする (Enable RSA Signature Hash)] : RSA 署名ハッシュを有効にするには、このチェックボックスをオンにします。RSA は暗号化の一種です。

- [IKE Policy] : IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [Manage] : [Configure IKEv1 Proposals] ダイアログボックスが開きます。
- [IPsec Proposal] : IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [Select] : IKEv2 接続の接続プロファイルにプロポーザルを割り当てることができる [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開きます。

この接続プロファイルには、次のパラメータもあります。

- [詳細 (Advanced)] > [クリプトマップエントリ (Crypto Map Entry)]。詳細については、[Site-to-Site 接続プロファイル、暗号マップエントリ \(94 ページ\)](#) を参照してください。

Site-to-Site トンネル グループ

ASDM ペインの [設定 (Configuration)] > [サイト間 VPN (Site-to-Site VPN)] > [詳細 (Advanced)] > [トンネルグループ (Tunnel Groups)] では、IPsec サイト間接続プロファイル (トンネルグループ) の属性を指定します。また、IKE ピアとユーザー認証パラメータの選択、IKE キープアライブ モニタリングの設定、およびデフォルト グループ ポリシーの選択も行うことができます。

- [Name] : このトンネルグループに割り当てられた名前を指定します。Edit機能の場合、このフィールドは表示専用です。
- [IKE Authentication] : IKE ピアの認証で使用する事前共有キーおよび ID 証明書パラメータを指定します。
 - [Pre-shared Key] : トンネルグループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Identity Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。
 - [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
 - [IKE Peer ID Validation] : IKE ピア ID の有効性をチェックするかどうかを指定します。デフォルトは Required です。
- [IPsec Enabling] : この接続プロファイルのグループ ポリシー、およびそのポリシーで指定したキー交換プロトコルを指定します。
 - [Group Policy Name] : この接続プロファイルに関連付けられているグループ ポリシーを指定します。
 - [Manage] : [Browse Remote Network] ダイアログボックスが開きます。このダイアログボックスでは、リモート ネットワークを選択できます。

- [Enable IKEv1] : 指定したグループ ポリシーでキー交換プロトコル IKEv1 をイネーブ
ルにします。
- [Enable IKEv2] : 指定したグループ ポリシーでキー交換プロトコル IKEv2 をイネーブ
ルにします。
- [IKEv1 Settings] タブ : IKEv1 の次の認証設定および暗号化設定を指定します。
 - [Pre-shared Key] : トンネルグループの事前共有キーの値を指定します。事前共有キー
の最大長は 128 文字です。
 - [Device Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。



(注) 一部のプロファイルは、エンドポイントがリモートアクセスまたは LAN-かどうかを判別できないことがあります。トンネルグループを判別できない場合、デフォルトで

```
tunnel-group-map default-group <tunnel-group-name>
```

に設定されます (デフォルト値は *DefaultRAGroup* です) 。

- [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイア
ログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書
の詳細の表示、および証明書の編集または削除を行うことができます。
- [IKE Policy] : IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定しま
す。
- [Manage] : [Configure IKEv1 Proposals] ダイアログボックスが開きます。
- [IPsec Proposal] : IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上
指定します。
- [IKEv2 Settings] タブ : IKEv2 の次の認証設定および暗号化設定を指定します。
 - [Local Pre-shared Key] : トンネルグループの事前共有キーの値を指定します。事前共
有キーの最大長は 128 文字です。
 - [Local Device Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定し
ます。
 - [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイア
ログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書
の詳細の表示、および証明書の編集または削除を行うことができます。
 - [Remote Peer Pre-shared Key] : トンネルグループのリモートピア事前共有キーの値を
指定します。事前共有キーの最大長は 128 文字です。
 - [Remote Peer Certificate Authentication] : この接続プロファイルの IKEv2 接続用の証明
書認証を許可するには、[Allowed] をオンにします。

- **[Manage]** : 証明書の表示や新規証明書の追加を実行できる **[Manage CA Certificates]** ダイアログが開きます。
 - **[IKE Policy]** : IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
 - **[Manage]** : **[Configure IKEv1 Proposals]** ダイアログボックスが開きます。
 - **[IPsec Proposal]** : IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
 - **[Select]** : IKEv2 接続の接続プロファイルにプロポーザルを割り当てることができる **[Select IPsec Proposals (Transform Sets)]** ダイアログボックスが開きます。
 - **[リモートピアポスト量子事前共有キー (Remote Peer Post Quantum Key)]** : 事前共有キーの代わりに、IKEv2 用のポスト量子事前共有キー (PPK) を指定するには、このチェックボックスをオンにします。PPK は、256 ビット 64 文字の 16 進数文字列です。

PPK は事前共有キーに似ており、IKEv2 を量子コンピュータの攻撃から保護します。
 - **[パスワードの表示 (Show Password)]** : このチェックボックスをオンにすると、PPK キーが表示されます。
 - **[リモートピアポスト量子キーID (Remote Peer Post Quantum Key Identity)]** : PPK の ID を指定します。
- **[IKE Keepalive]** : IKE キープアライブ モニタリングをイネーブルにし、設定を行います。次の属性の中から 1 つだけ選択できます。
 - **[Disable Keep Alives]** : IKE キープアライブをイネーブルまたはディセーブルにします。
 - **[Monitor Keep Alives]** : IKE キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、**[Confidence Interval]** フィールドと **[Retry Interval]** フィールドが利用できるようになります。
 - **[Confidence Interval]** : IKE キープアライブの信頼間隔を指定します。これは、ASA がキープアライブモニタリングを開始するまでに、ピアがアイドル状態を継続できる秒数です。最小 10 秒、最大 300 秒です。リモートアクセスグループのデフォルトは 10 秒です。
 - **[Retry Interval]** : IKE キープアライブのリトライ間の待機秒数を指定します。デフォルト値は 2 秒です。
 - **[Head end will never initiate keepalive monitoring]** : 中央サイトの ASA がキープアライブモニタリングを開始しないように指定します。

Site-to-Site 接続プロファイル、暗号マップ エントリ

このダイアログボックスでは、現在の Site-to-Site 接続プロファイルの暗号パラメータを指定します。

- [Priority] : 一意のプライオリティ (1 ~ 65,543、1 が最高のプライオリティ)。IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモートピアに送信します。リモートピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。
- [Perfect Forward Secrecy] : 特定の IPsec SA のキーが他の秘密情報 (他のキーなど) から導出されたものでないことを保証します。PFS により、攻撃者がキーを突破できたとしても、そのキーから他のキーを導出できないようにします。PFS をイネーブルにすると、Diffie-Hellman Group リストがアクティブになります。
 - [Diffie-Hellman Group] : 2 つの IPsec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1 (768 ビット)、Group 2 (1024 ビット)、および Group 5 (1536 ビット) の中から選択します。
- [Enable NAT-T] : このポリシーの NAT Traversal (NAT-T) をイネーブルにします。これにより IPsec ピアは、NAT デバイスを介してリモートアクセスと LAN-to-LAN の両方の接続を確立できます。
- [Enable Reverse Route Injection] : リモートトンネルのエンドポイントによって保護されているネットワークとホストのルーティングプロセスに、スタティックルートが自動的に挿入されるようにすることができます。
- [Security Association Lifetime] : セキュリティアソシエーション (SA) の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
 - [Time] : 時 (hh)、分 (mm)、および秒 (ss) 単位で SA のライフタイムを指定します。
 - [Traffic Volume] : キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロードデータのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。
- [Static Crypto Map Entry Parameters] : ピア IP アドレスが Static に指定されている場合に、次の追加パラメータを指定します。
 - [Connection Type] : 許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。
 - [Send ID Cert. Chain] : 証明書チェーン全体の送信をイネーブルにします。
 - [IKE Negotiation Mode] : SA、Main、または Aggressive の中から、セットアップでキー情報を交換するときのモードを設定します。ネゴシエーションの発信側が使用するモードも設定されます。応答側は自動ネゴシエーションします。Aggressive モードは

高速で、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。Main モードは低速で、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。このモードはより安全性が高く、デフォルトで選択されています。[Aggressive] を選択すると、[Diffie-Hellman Group] リストがアクティブになります。

- [Diffie-Hellman Group] : 2 つの IPsec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1 (768 ビット)、Group 2 (1024 ビット)、および Group 5 (1536 ビット) の中から選択します。

CA 証明書の管理

CA 証明書の管理は、リモートアクセス VPN とサイト間 VPN に適用されます。

- Site-to_site の場合 : [IKE Peer Authentication] の [Manage] をクリックすると、[Manage CA Certificates] ダイアログボックスが開きます。
- リモートアクセス VPN では、[Certificate Management] > [CA Certificates] をクリックします。

このダイアログボックスを使用して、IKE ピア認証で使用可能な CA 証明書のリストのエントリを、表示、追加、編集、および削除します。[Manage CA Certificates] ダイアログボックスには、証明書の発行先、証明書の発行元、証明書の有効期限、および利用データなど、現在設定されている証明書の情報が一覧表示されます。

- [Add or Edit] : [Install Certificate] ダイアログボックスまたは [Edit Certificate] ダイアログボックスが開きます。これらのダイアログボックスでは、証明書の情報を指定し、証明書をインストールできます
- [Show Details] : テーブルで選択する証明書の詳細情報を表示します。
- [Delete] : 選択した証明書をテーブルから削除します。確認されず、やり直しもできません。

Site-to-Site 接続プロファイル、証明書のインストール

このダイアログボックスを使用して、新しい CA 証明書をインストールします。次のいずれかの方法で証明書を取得できます。

- 証明書ファイルを参照してファイルからインストールします。
- 事前取得済みの PEM 形式の証明書テキストをこのダイアログボックス内のボックスに貼り付けます。
- [Use SCEP] : Simple Certificate Enrollment Protocol (SCEP) の使用を指定します。証明書サービスのアドオンは、Windows Server 2003 ファミリで実行されます。SCEP プロトコルのサポートを提供し、これによりシスコのルータおよび他の中間ネットワーク デバイスは、証明書を取得できます。

- [SCEP URL: http://] : SCEP 情報のダウンロード元の URL を指定します。
- [Retry Period] : SCEP クエリー間の必須経過時間を分数で指定します。
- [Retry Count] : リトライの最大許容回数を指定します。
- [More Options] : [Configure Options for CA Certificate] ダイアログボックスが開きます。

このダイアログボックスを使用して、この IPsec リモート アクセス接続の CA 証明書の取得に関する詳細を指定します。このダイアログボックスに含まれるダイアログボックスは、[Revocation Check]、[CRL Retrieval Policy]、[CRL Retrieval Method]、[OCSP Rules]、および [Advanced] です。

[Revocation Check] ダイアログボックスは、CA 証明書失効確認に関する情報を指定するために使用します。

- オプション ボタンにより、失効状態について証明書をチェックするかどうかを指定します。[Do not check certificates for revocation] または [Check Certificates for revocation] を選択します。
- [Revocation Methods area] : 失効チェックに使用する方法 (CRL または OCSP) 、およびそれらの方法を使用する順序を指定できます。いずれか一方または両方の方法を選択できます。

Cisco Secure Client イメージの AnyConnect VPN モジュール

[設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [AnyConnect クライアントソフトウェア (Client Software)] ペインに、ASDM で設定された AnyConnect クライアントイメージが一覧表示されます。

[AnyConnect クライアントイメージ (AnyConnect Client Image)] テーブル : ASDM で設定されたパッケージファイルが表示されます。ASA がリモート PC にイメージをダウンロードする順序を設定できます。

- [追加 (Add)] : [AnyConnect クライアントイメージの追加 (Add AnyConnect Client Image)] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルをクライアントイメージファイルとして指定したり、フラッシュメモリから、クライアントイメージとして指定するファイルを参照したりできます。また、ファイルをローカル コンピュータからフラッシュメモリにアップロードすることもできます。
- [置換 (Replace)] : [AnyConnect クライアントイメージの置換 (Replace Image)] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルをクライアントイメージとして指定して、[SSL VPN クライアントイメージ (SSL VPN Client Image)] テーブルで選択したイメージと置換できます。また、ファイルをローカル コンピュータからフラッシュメモリにアップロードすることもできます。

- [Delete] : テーブルからイメージを削除します。イメージを削除しても、パッケージ ファイルはフラッシュから削除されません。
- [Move Up] および [Move Down] : 上矢印と下矢印を使用して、ASA がリモート PC にクライアントイメージをダウンロードする順序を変更します。テーブルの一番上にあるイメージを最初にダウンロードします。このため、最もよく使用するオペレーティングシステムで使用されるイメージを一番上に移動する必要があります。

Cisco Secure Client イメージの AnyConnect VPN モジュール、追加/置換

このペインでは、ASA フラッシュメモリ上のファイルの名前を指定して、そのファイルを AnyConnect クライアントイメージとして追加したり、テーブルにすでに記載されているイメージと置換することができます。また、識別するファイルをフラッシュメモリから参照したり、ローカル コンピュータからファイルをアップロードしたりすることもできます。

- [Flash SVC Image] : SSL VPN クライアント イメージとして識別する、フラッシュ メモリ内のファイルを指定します。
- [Browse Flash] : フラッシュメモリに格納されているすべてのファイルを参照できる [Browse Flash Dialog] ダイアログボックスを表示します。
- [Upload] : [Upload Image] ダイアログボックスが表示されます。このダイアログボックスでは、クライアントイメージとして指定するファイルをローカル PC からアップロードできます。
- [Regular expression to match user-agent] : ASA が、ブラウザから渡された User-Agent 文字列との照合に使用する文字列を指定します。モバイルユーザーの場合、この機能を使用してモバイルデバイスの接続時間を短縮できます。ブラウザはASAに接続するときに、HTTP ヘッダーに User-Agent 文字列を含めます。ASA が文字列を受信し、その文字列がいずれかのイメージ用に設定された式と一致すると、他のクライアントイメージはテストされず、一致したイメージがただちにダウンロードされます。

Cisco Secure Client イメージの AnyConnect VPN モジュール、イメージのアップロード

このペインでは、ローカルコンピュータまたはセキュリティアプライアンスのフラッシュメモリに格納されている、AnyConnect クライアントイメージとして識別するファイルのパスを指定できます。ローカルコンピュータまたはセキュリティアプライアンスのフラッシュメモリから、識別するファイルを参照できます。

- [Local File Path] : ローカルコンピュータに格納されている、SSL VPN クライアントイメージとして識別するファイルの名前を指定します。
- [Browse Local Files] : [Select File Path] ダイアログボックスが表示されます。このダイアログボックスでは、ローカル コンピュータ上のすべてのファイルを表示し、クライアントイメージとして識別するファイルを選択できます。
- [Flash File System Path] : セキュリティアプライアンスのフラッシュメモリに格納されている、SSL VPN クライアントイメージとして識別するファイルの名前を指定します。

- [Browse Flash] : [Browse Flash] ダイアログボックスが表示されます。このダイアログボックスでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。
- [Upload File] : ファイルのアップロードを開始します。

AnyConnect クライアント外部ブラウザ SAML パッケージ

[設定 (Configuration)] > [アクセスVPNの削除 (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > > [AnyConnect外部ブラウザ (AnyConnect External Browser)] ペインには、AnyConnect クライアント SAML シングルサインオン (SSO) 認証に使用できる AnyConnect クライアント 外部ブラウザパッケージが一覧表示されます。

AnyConnect クライアント 外部ブラウザパッケージイメージ : ASDM で設定された外部ブラウザパッケージファイルを表示します。

- [追加 (Add)] : [AnyConnect クライアント外部ブラウザイメージの追加 (Add AnyConnect External Browser Image)] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルを外部パッケージイメージファイルとして指定したり、フラッシュメモリから、外部ブラウザパッケージファイルとして指定するファイルを参照したりできます。
- [置き換え (Replace)] : [AnyConnect クライアント外部ブラウザパッケージの置き換え (Replace AnyConnect External Browser Package)] ダイアログボックスが表示されます。ここでは、フラッシュメモリ内のファイルを外部ブラウザパッケージとして指定して、既存のパッケージファイルを置き換えることができます。
- [削除 (Delete)] : 外部ブラウザパッケージファイルをテーブルから削除します。イメージを削除しても、パッケージ ファイルはフラッシュから削除されません。
- [上に移動 (Move Up)] および [下に移動 (Move Down)] : 上矢印と下矢印を使用して、ASA がリモート PC に外部ブラウザパッケージをダウンロードする順序を変更します。

[AnyConnect クライアント外部ブラウザSAMLパッケージイメージ、追加/置き換え (AnyConnect Client External Browser SAML Package Images, Add/Replace)]

このペインでは、ASA フラッシュメモリ上のファイルの名前を指定して、そのファイルを AnyConnect クライアント 外部ブラウザパッケージイメージとして追加したり、テーブルにすでに記載されているイメージと置換したりすることができます。また、識別するファイルをフラッシュメモリから参照したり、ローカル コンピュータからファイルをアップロードしたりすることもできます。

- [AnyConnect クライアント外部ブラウザパッケージ (AnyConnect Client External Browser Package)] : 外部ブラウザパッケージイメージとして識別するフラッシュメモリ内のファイルを指定します。

- [フラッシュの参照 (BrowseFlash)]: フラッシュメモリ上のすべてのファイルを参照できる [フラッシュの参照 (Browse Flash)] ダイアログボックスが表示されます。
- [アップロード (Upload)]: [イメージのアップロード (Upload Image)] ダイアログボックスが表示されます。このダイアログボックスでは、外部ブラウザパッケージイメージとして指定するファイルをローカル PC からアップロードできます。

[AnyConnect クライアント外部ブラウザSAMLパッケージイメージ、イメージのアップロード (AnyConnect External Browser SAML Package Images, Upload Image)]

このペインでは、ローカルコンピュータまたはセキュリティアプライアンスのフラッシュメモリに格納されている、AnyConnect クライアント イメージとして識別するファイルのパスを指定できます。ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュメモリから、識別するファイルを参照できます。

- [ローカルファイルパス (Local File Path)]: ローカルコンピュータに格納されている、外部ブラウザパッケージイメージとして識別するファイルの名前を指定します。
- [ローカルファイルの参照 (Browse Local Files)]: [ファイルパスの選択 (Select File Path)] ダイアログボックスが表示されます。このダイアログボックスでは、ローカルコンピュータ上のすべてのファイルを表示し、外部ブラウザパッケージイメージとして識別するファイルを選択できます。
- [フラッシュファイルのシステムパス (Flash File System Path)]: セキュリティアプライアンスのフラッシュメモリに格納されている、外部ブラウザパッケージイメージとして識別するファイルの名前を指定します。
- [フラッシュの参照 (BrowseFlash)]: [フラッシュの参照 (BrowseFlash)] ダイアログボックスが表示されます。このダイアログボックスでは、セキュリティアプライアンスのフラッシュメモリに格納されているすべてのファイルを表示し、外部ブラウザパッケージイメージとして識別するファイルを選択できます。
- [ファイルのアップロード (Upload File)]: ファイルのアップロードを開始します。

AnyConnect クライアントVPN 接続の設定

AnyConnect クライアント接続の注意事項と制約事項

セッショントークンの推奨事項

ASA が AnyConnect クライアントからの VPN 接続要求を認証すると、セキュリティを強化するためにセッショントークンがクライアントに返されます。AnyConnect 4.9 (MR1) 以降、ASA と AnyConnect クライアントは、セッショントークンのセキュリティを強化するメカニズムをサポートします。トークンセキュリティをサポートしていない AnyConnect クライアントバー

ジョンからの接続試行を拒否するように DAP ルールを設定できます。DAP を使用してセッション トークンのセキュリティを確認する を参照してください。

AnyConnect クライアント プロファイルの設定

ASA は、すべての AnyConnect クライアント ユーザーにグローバルに AnyConnect クライアント プロファイルを展開するか、ユーザーのグループポリシーに基づいて展開するように設定できます。通常、ユーザーは、インストールされている AnyConnect クライアント モジュールごとに1つのクライアントプロファイルを持ちます。ユーザーに複数のプロファイルを割り当てることもできます。たとえば、複数の場所で作業するユーザーには、複数のプロファイルが必要になることがあります。一部のプロファイル設定（SBL など）は、グローバル レベルで接続を制御します。その他の設定は、特定のホストに固有であり、選択されたホストにより異なります。

AnyConnect クライアントプロファイルの作成と展開、およびクライアント機能の制御の詳細については、『AnyConnect VPN Client Administrator Guide』を参照してください。

クライアントプロファイルは、[設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [AnyConnect クライアントプロファイル (Profile)] で設定します。

[追加/インポート (Add/Import)] : [AnyConnect クライアントプロファイルの追加 (Add AnyConnect Profiles)] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルをプロファイルとして指定したり、フラッシュメモリを参照してプロファイルとして指定するファイルを検索したりできます。また、ファイルをローカルコンピュータからフラッシュメモリにアップロードすることもできます。

- [プロファイル名 (Profile Name)] : グループポリシーの AnyConnect クライアント プロファイルを指定します。
- [Profile Usage] : 最初に作成されたときにプロファイルに割り当てられた用途 (VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ISE ポスチャ、AMP イネーブラ、ネットワーク可視性モジュール、Umbrella Roaming Security、または管理 VPN トンネル) を表示します。ASDM が、XML ファイルで指定された用途を認識しない場合、ドロップダウンリストが選択可能になり、用途タイプを手動で選択できます。
- [Profile Location] : ASA のフラッシュメモリ内のプロファイルファイルへのパスを指定します。このファイルが存在しない場合、ASA はプロファイルテンプレートに基づいてファイルを作成します。
- [Group Policy] : プロファイルのグループポリシーを指定します。プロファイルは、AnyConnect クライアント とともにこのグループポリシーに属しているユーザーにダウンロードされます。

[編集 (Edit)] : [SSL VPNクライアントプロファイルの編集 (Edit SSL VPN Client Profiles)] ウィンドウが表示されます。このウィンドウでは、プロファイルに含まれている AnyConnect クライアント 機能の設定を変更できます。

[エクスポート (Export)]

- [Device Profile Path] : プロファイル ファイルのパスおよびファイル名を表示します。
- [Local Path] : パスとファイル名を指定してプロファイル ファイルをエクスポートします。
- [Browse Local] : ローカル デバイス ファイル システムを参照するには、これをクリックしてウィンドウを起動します。

[Delete] : テーブルからプロファイルを削除します。プロファイルを削除しても、XML ファイルはフラッシュから削除されません。

[AnyConnect クライアントプロファイル (AnyConnect Profiles)] テーブル : AnyConnect クライアント プロファイルとして指定された XML ファイルを表示します。

AnyConnect クライアント トラフィックに対するネットワークアドレス変換の免除

ネットワークアドレス変換 (NAT) を実行するように ASA を設定した場合は、AnyConnect クライアント、内部ネットワーク、および DMZ の企業リソースが相互に接続を開始できるように、リモートアクセス AnyConnect クライアント トラフィックを変換の対象外にする必要があります。AnyConnect クライアント トラフィックを変換の対象外にできないと、AnyConnect クライアントおよび他の企業リソースが通信できなくなります。

「アイデンティティ NAT」 (「NAT 免除」とも呼ばれている) によりアドレスを自らに変換できます。これにより効果的に NAT が回避されます。アイデンティティ NAT は 2 つのアドレスプール、アドレスプールとサブネットワーク、または 2 つのサブネットワーク間で適用できます。

この手順は、例にあるネットワーク トポロジの次の仮定のネットワーク オブジェクト間でアイデンティティ NAT を設定する方法を示しています。それらは、Engineering VPN アドレスプール、Sales VPN アドレスプール、ネットワーク内、DMZ ネットワーク、およびインターネットです。アイデンティティ NAT 設定ではそれぞれ、NAT 規則が 1 つ必要です。

表 4: VPN クライアントのアイデンティティ NAT を設定するネットワーク アドレス アドレッシング

ネットワークまたはアドレスプール	ネットワーク名またはアドレスプール名	アドレス範囲
内部ネットワーク	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN アドレスプール	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN アドレスプール	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ ネットワーク	DMZ-network	192.168.1.0 - 192.168.1.255

手順

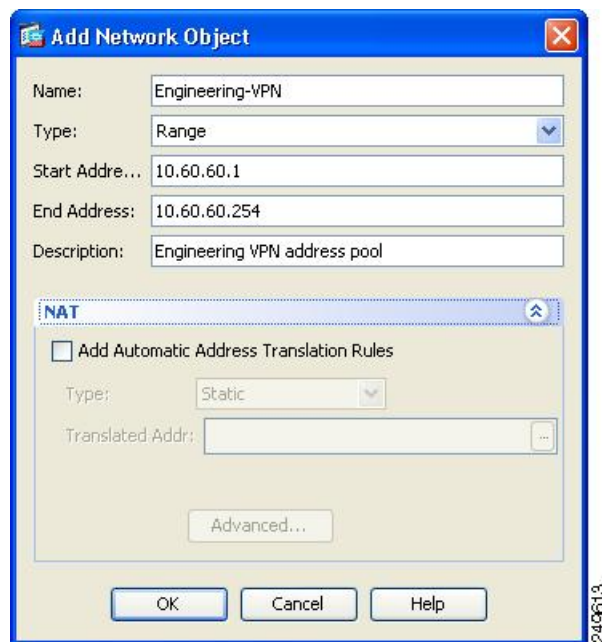
- ステップ 1** ASDM にログインし、[Configuration] > [Firewall] > [NAT Rules] に移動します。
- ステップ 2** Engineering VPN アドレス プールのホストが Sales VPN アドレス プールのホストに接続できるよう、NAT 規則を作成します。ASA が Unified NAT テーブルの他の規則よりも先にこの規則を評価するように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] に移動します。
- (注) NAT ルールはトップダウン方式で最初に一致したルールから順に適用されます。ASA によりいったんパケットが特定の NAT 規則と一致すると、それ以上評価は行われません。ASA が NAT 規則を早まって広範な NAT 規則に一致しないよう、Unified NAT テーブルの先頭に最も固有の NAT 規則を配置することが重要です。

図 1: [Add NAT Rule] ダイアログ ボックス

- a) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。
- [Source Interface:] Any
 - [Destination Interface:] Any
 - [Source Address:] [Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクトタイプをアドレスの [Range] として定義します。自動アドレス トランスレーションルールは追加しないでください。
 - [Destination Address:] [Destination Address] ブラウズ ボタンをクリックし、Sales VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクトタイプ

をアドレスの [Range] として定義します。自動アドレス トランスレーションルールは追加しないでください。

図 2: VPN アドレス プールのネットワーク オブジェクトの作成



- b) [Action Translated Packet] エリアで、次のフィールドを設定します。
- [Source NAT Type:] Static
 - [Source Address:] Original
 - [Destination Address:] Original
 - [Service:] Original
- c) [Options] エリアで、次のフィールドを設定します。
- [Enable rule] をオンにします。
 - [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
 - [Direction:] Both
 - [Description:] 規則の説明を入力します。
- d) [OK] をクリックします。
- e) [Apply] をクリックします。

CLI の例 :

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN  
Sales-VPN
```

f) [Send] をクリックします。

ステップ 3 ASA が NAT を実行しているときに、同じ VPN プール内の 2 つのホストが互いに接続できるように、またはそれらのホストが VPN トンネル経由でインターネットに接続できるように、[Enable traffic between two or more hosts connected to the same interface] オプションをイネーブルにする必要があります。これを行うには、ASDM で [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] を選択します。[Interface] パネルの下の [Enable traffic between two or more hosts connected to the same interface] をオンにして、[Apply] をクリックします。

CLI の例 :

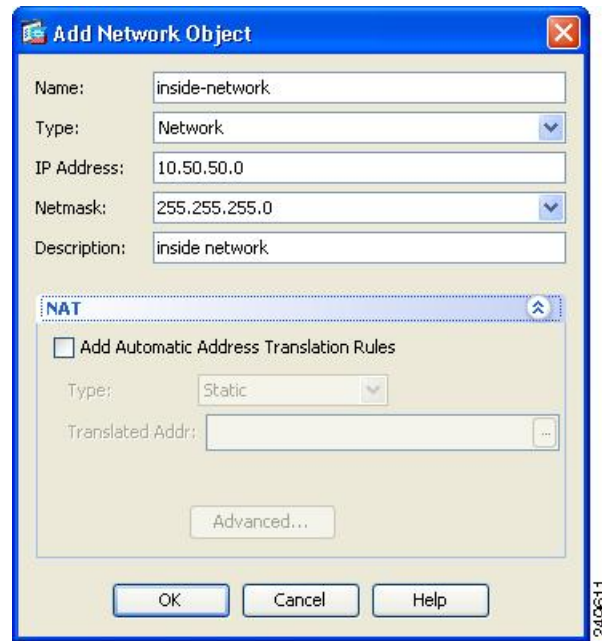
```
same-security-traffic permit inter-interface
```

ステップ 4 Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。上記で規則を作成したときと同様にこの規則を作成します。ただし、[Match criteria: Original Packet] エリアで、Engineering VPN アドレス プールを送信元と宛先の両方のアドレスとして指定します。

ステップ 5 Engineering VPN リモートアクセスクライアントが「内部」ネットワークに到達できるよう NAT 規則を作成します。この規則が他の規則よりも先に処理されるように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。

a) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、内部ネットワークを表すネットワーク オブジェクトを作成します。オブジェクトタイプをアドレスの [Network] として定義します。自動アドレス トランスレーションルールは追加しないでください。
- [Destination Address:] [Destination Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。

図 3: *inside-network* オブジェクトの追加

- b) [Action Translated Packet] エリアで、次のフィールドを設定します。
- [Source NAT Type:] Static
 - [Source Address:] Original
 - [Destination Address:] Original
 - [Service:] Original
- c) [Options] エリアで、次のフィールドを設定します。
- [Enable rule] をオンにします。
 - [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
 - [Direction:] Both
 - [Description:] 規則の説明を入力します。
- d) [OK] をクリックします。
- e) [Apply] をクリックします。

CLI の例

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

ステップ 6 ステップ 5 の方法に従って新しい規則を作成し、Engineering VPN アドレスプールと DMZ ネットワーク間の接続のアイデンティティ NAT を設定します。DMZ ネットワークを送信元アドレス、Engineering VPN アドレスプールを宛先アドレスとして使用します。

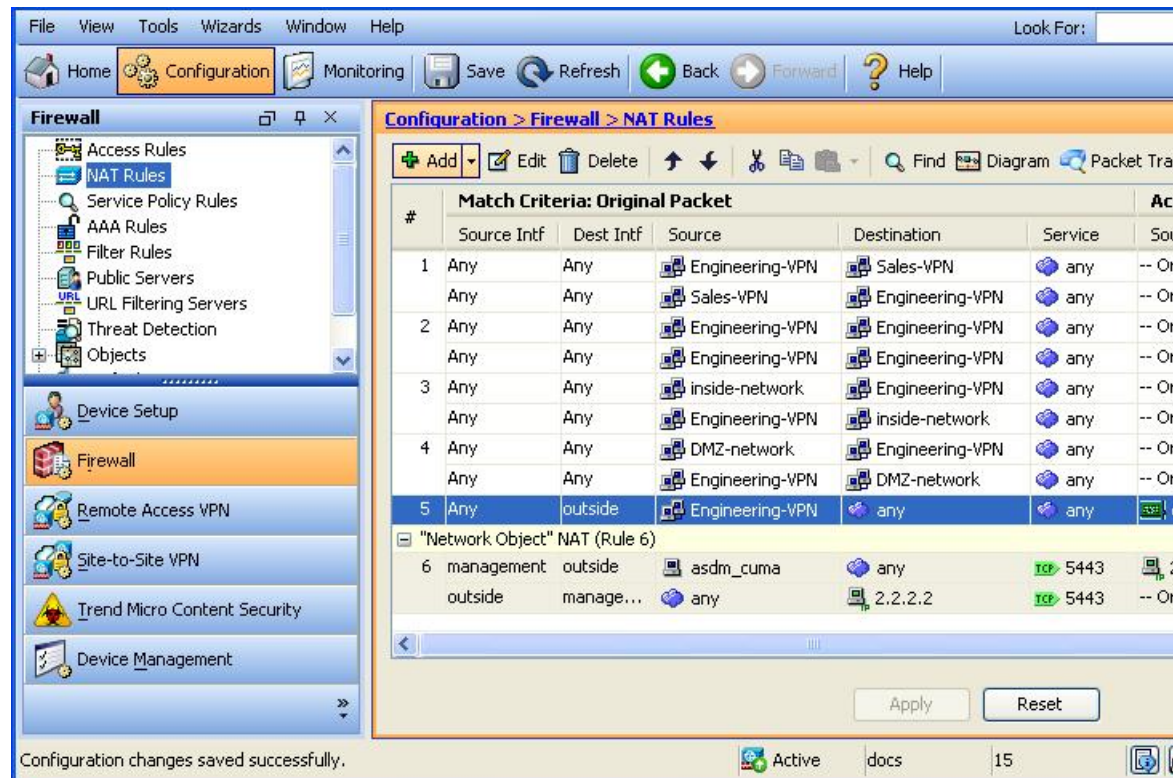
ステップ 7 新しい NAT 規則を作成し、Engineering VPN アドレスプールがトンネル経由でインターネットにアクセスできるようにします。この場合、アイデンティティ NAT は使用しません。送信元アドレスをプライベートアドレスからインターネットルーティング可能なアドレスに変更するためです。この規則を作成するには、次の手順に従います。

- a) この規則が他の規則よりも先に処理されるように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。
- b) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。
 - [Source Interface:] Any
 - [Destination Interface:] Any。 [Action: Translated Packet] エリアの [Source Address] で [outside] を選択すると、このフィールドに自動的に「outside」が入力されます。
 - [Source Address] : [Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレスプールを表すネットワーク オブジェクトを選択します。
 - [Destination Address:] Any
- c) [Action Translated Packet] エリアで、次のフィールドを設定します。
 - [Source NAT Type:] Dynamic PAT (Hide)
 - [Source Address:] [Source Address] ブラウズ ボタンをクリックして、outside インターフェイスを選択します。
 - [Destination Address:] Original
 - [Service:] Original
- d) [Options] エリアで、次のフィールドを設定します。
 - [Enable rule] をオンにします。
 - [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
 - [Direction:] Both
 - [Description:] 規則の説明を入力します。
- e) [OK] をクリックします。
- f) [Apply] をクリックします。

CLI の例 :

```
nat (any,outside) source dynamic Engineering-VPN interface
```

図 4: Unified NAT テーブル



- ステップ 8** Engineering VPN アドレス プールがそのプール自体、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネットに到達するように設定した後に、Sales VPN アドレス プールについて同じプロセスを繰り返す必要があります。アイデンティティ NAT を使用して、Sales VPN アドレス プールトラフィックが、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネット間のネットワークアドレス変換の対象外となるようにします。
- ステップ 9** ASA の [File] メニューで [Save Running Configuration to Flash] を選択し、アイデンティティ NAT 規則を実装します。

AnyConnect クライアント HostScan

AnyConnect クライアント HostScan (現在は Cisco Secure Firewall ポスチャと呼ばれています) により、Secure Client) はホストにインストールされているオペレーティングシステム、マルウェア対策、ファイアウォールの各ソフトウェアを識別できます。この情報は、Cisco Secure Firewall ポスチャ/HostScan アプリケーションによって収集されます。ポスチャアセスメントでは、ホストに Secure Firewall ポスチャ/HostScan がインストールされている必要があります。

ASDM UI は動的であり、HostScan がロードされている場合は HostScan が反映されます。Secure Firewall ポスチャがロードされると、Secure Firewall ポスチャが反映されます。実行しているバージョンによって名前は異なります。

HostScan/Secure Firewall ポスチャの前提条件

AnyConnect クライアントを Secure Firewall Posture/HostScan モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

SCEP 認証機能を使用するには、Secure Firewall Posture/HostScan をインストールする必要があります。

Secure Firewall Posture/HostScan のインストールでサポートされるオペレーティングシステムについては、『[Supported VPN Platforms, Cisco ASA Series](#)』を参照してください。

AnyConnect クライアント HostScan/Secure Firewall ポスチャのライセンス

Secure Firewall ポスチャ/HostScan のライセンス要件は次のとおりです。

- 基本的な HostScan/Secure Firewall ポスチャの AnyConnect クライアントの利点 (Apex)。
- 修復には、Advanced Endpoint Assessment ライセンスが必要です。

HostScan パッケージ

HostScan パッケージを ASA にスタンドアロンパッケージ `hostscan-version.pkg` としてロードすることができます。このファイルには、HostScan ソフトウェアとともに、HostScan ライブラリおよびサポート表が含まれています。

HostScan/Secure Firewall ポスチャのインストールまたはアップグレード

この手順では、ASDM を使用して、HostScan/Secure Firewall ポスチャパッケージをインストールまたはアップグレードし、有効にします。ASDM UI は動的であり、HostScan がロードされている場合は HostScan が反映されます。Secure Firewall ポスチャがロードされると、Secure Firewall ポスチャが反映されます。実行しているバージョンによって名前は異なります。

始める前に



- (注) HostScan バージョン 4.3.x 以前から 4.6.x 以降にアップグレードしようとしている場合、以前に確立した既存の AV/AS/FW DAP ポリシーおよび LUA スクリプトがすべて HostScan 4.6.x 以降と非互換であるという事実に起因するエラー メッセージが表示されます。

設定を適応させるために実行する必要があるワнтаイト移行手順が存在します。この手順では、このダイアログボックスを閉じて、この設定を保存する前に HostScan 4.4.x と互換になるように設定を移行します。この手順を中止し、『[AnyConnect クライアント HostScan 4.3.x to 4.6.x Migration Guide](#)』で詳細な手順を参照してください。つまり、移行するには ASDM DAP のポリシー ページに移動して、互換性のない AV/AS/FW 属性を確認して手動で削除してから、LUA スクリプトを確認し、書き換える必要があります。

手順

- ステップ 1** バージョン 5 を使用している場合は、secure-firewall-posture-version-k9.pkg ファイルをコンピュータにダウンロードします。バージョン 4.x の場合、ファイルは hostscan_version-k9.pkg です。
- ステップ 2** ASDM を開いて [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [Cisco Secure Firewall 用 ポスチャ (Posture (for Secure Firewall))] > [ポスチャ イメージ (Posture Image)] を選択します。HostScan 4.x バージョンを使用している場合、パスは [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [Secure Desktop Manager] > [ホスト スキャン イメージ (Host Scan Image)] になります。
- ステップ 3** [アップロード (Upload)] をクリックして、HostScan/Secure Firewall ポスチャ パッケージのコピーをコンピュータから ASA のドライブに転送する準備を行います。
- ステップ 4** [イメージのアップロード (Upload Image)] ダイアログボックスで [ローカルファイルの参照 (Browse Local Files)] をクリックして、ローカルコンピュータ上の HostScan/Secure Firewall ポスチャ パッケージを検索します。
- ステップ 5** 先ほどダウンロードした hostscan_version-k9.pkg ファイル、または secure-firewall-posture-version-k9.pkg ファイルを選択し、[選択 (Select)] をクリックします。[ローカルファイルパス (Local File Path)] フィールドと [フラッシュファイルシステムパス (Flash File System Path)] フィールドで選択したファイルのパスは、HostScan/Secure Firewall パッケージのアップロード先のパスを反映しています。ASA に複数のフラッシュ ドライブがある場合は、別のフラッシュ ドライブを示すように [Flash File System Path] を編集できます。
- ステップ 6** [Upload File] をクリックします。ASDM によって、ファイルのコピーがフラッシュ カードに転送されます。情報ダイアログボックスに、ファイルがフラッシュに正常にダウンロードされたことが表示されます。
- ステップ 7** [OK] をクリックします。
- ステップ 8** [アップロードしたイメージの使用 (Use Uploaded Image)] ダイアログで [OK] をクリックして、現在のイメージとしてアップロードした HostScan/Secure Firewall ポスチャ パッケージ ファイルを使用します。

- ステップ 9 [HostScanを有効化 (Enable HostScan)]または[ポスチャイメージを有効化 (Enable Posture Image)]がオンになっていない場合はオンにします。
- ステップ 10 [Apply] をクリックします。
- ステップ 11 [File] メニューから [Save Running Configuration To Flash] を選択します。

HostScan/Secure Firewall ポスチャのアンインストール

HostScan/Secure Firewall ポスチャパッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、HostScan/Secure Firewall ポスチャが有効になっている場合でも ASA による HostScan/Secure Firewall ポスチャパッケージの展開が回避されません。HostScan/Secure Firewall ポスチャをアンインストールしても、HostScan/Secure Firewall ポスチャパッケージはフラッシュドライブから削除されません。

手順

- ステップ 1 ASDM で、[設定 (Configuration)]>[リモートアクセスVPN (Remote Access VPN)]>[ポスチャ (Secure Firewall用) (Posture for Secure Firewall)]>[ポスチャイメージ (Posture Image)]に移動して、Secure Firewall ポスチャをアンインストールします。AnyConnect バージョン 4.x を使用していて、HostScan をアンインストールする場合は、[設定 (Configuration)]>[リモートアクセスVPN (Remote Access VPN)]>[Secure Desktop Manager]>[ホストスキャンイメージ (Host Scan Image)]に移動します。
- ステップ 2 [Uninstall] をクリックし、確認のために [Yes] をクリックします。
- ステップ 3 [Uninstall] をクリックします。

グループポリシーへの AnyConnect クライアント 機能モジュールの割り当て

次の手順で、AnyConnect クライアント 機能モジュールとグループポリシーを関連付けます。VPN ユーザーが ASA に接続するときに、ASA はこれらの AnyConnect クライアント 機能モジュールをエンドポイントコンピュータにダウンロードしてインストールします。

始める前に

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は hostname(config)# プロンプトを表示します。

手順

ステップ 1 ネットワーク クライアント アクセス用の内部グループ ポリシーを追加します。

group-policy name internal

例 :

```
hostname (config) # group-policy PostureModuleGroup internal
```

ステップ 2 新しいグループ ポリシーを編集します。このコマンドを入力した後は、グループ ポリシー コンフィギュレーション モードのプロンプト `hostname(config-group-policy)#` が表示されます。

group-policy name attributes

例 :

```
hostname (config) # group-policy PostureModuleGroup attributes
```

ステップ 3 グループポリシー `webvpn` コンフィギュレーションモードを開始します。このコマンドを入力した後は、次に示す ASA のプロンプトが表示されます。 `hostname(config-group-webvpn)#`

webvpn

ステップ 4 グループ内のすべてのユーザーに AnyConnect クライアント 機能モジュールがダウンロードされるように、グループポリシーを設定します。

anyconnect modules value AnyConnect モジュール 名

`anyconnect module` コマンドの `value` には、次の値の 1 つ以上を指定することができます。複数のモジュールを指定する場合は、値をカンマで区切ります。

値	AnyConnect モジュール/機能名
dart	AnyConnect DART (診断およびレポートツール)
vpngina	AnyConnect SBL (ログイン前の起動)
ポスチャ	Secure Firewall ポスチャ/HostScan
nam	AnyConnect ネットワーク アクセス マネージャ
none	グループ ポリシーからすべての AnyConnect モジュールを削除する場合に使用します。
profileMgmt	AnyConnect 管理トンネル VPN

例 :

```
hostname (config-group-webvpn) # anyconnect modules value websecurity,telemetry,posture
```

モジュールの 1 つを削除するには、保持したいモジュールの値だけを指定したコマンドを再送信します。たとえば、このコマンドは `Web セキュリティ` モジュールを削除します。

```
hostname (config-group-webvpn) # anyconnect modules value telemetry,posture
```

ステップ 5 実行コンフィギュレーションをフラッシュメモリに保存します。

新しいコンフィギュレーションが正常にフラッシュメモリに保存されると、[OK] というメッセージが表示され、次に示す ASA のプロンプトが表示されます。hostname(config-group-webvpn)#
write memory

HostScan/Secure Firewall ポスチャ関連資料

HostScan/Secure Firewall ポスチャがエンドポイントコンピュータからポスチャクレデンシャルを収集した後は、情報を活用するために、ダイナミック アクセス ポリシーの設定、Lua の式の使用などのサブジェクトを理解する必要があります。

これらのトピックの詳細については、『[Cisco Adaptive Security Device Manager Configuration Guides](#)』を参照してください。また、AnyConnect クライアントでの HostScan/Secure Firewall ポスチャの動作の詳細については、『[Cisco Secure Client \(including AnyConnect\) Administrator Guide](#)』を参照してください。

Secure Client ソリューション

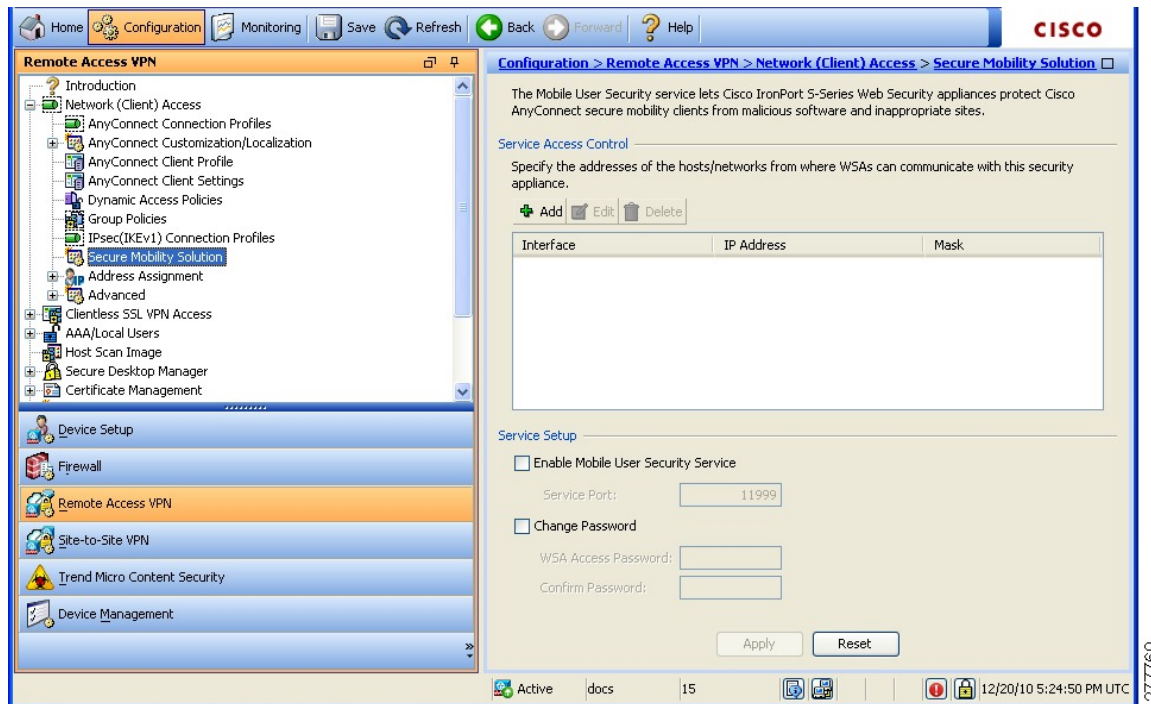
セキュアクライアントは、従業員の移動時に企業の利益と資産をインターネットの脅威から保護します。セキュアクライアントにより Cisco IronPort S シリーズ Web セキュリティアプライアンスはセキュアクライアントをスキャンでき、クライアントを悪意あるソフトウェアや不適切なサイトから確実に保護します。クライアントは、Cisco IronPort S シリーズ Web セキュリティアプライアンス保護がイネーブルになっているか定期的に確認します。



(注) この機能には、セキュアクライアント Secure Client ライセンスサポートを提供する Cisco IronPort Web セキュリティアプライアンスのリリースが必要です。また、セキュリティクライアント機能をサポートする AnyConnect クライアント リリースが必要です。AnyConnect 3.1 以降はこの機能をサポートしていません。

セキュア モビリティ ソリューションを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Secure Mobility Solution] の順に選択します。

図 5: [Mobile User Security] ウィンドウ



- [Service Access Control] : WSA の通信元となるホストまたはネットワーク アドレスを指定します。
 - [Add] : 選択した接続の [Add MUS Access Control Configuration] ダイアログボックスが開きます。
 - [Edit] : 選択した接続の [Edit MUS Access Control Configuration] ダイアログボックスが開きます。
 - [Delete] : 選択した接続をテーブルから削除します。確認されず、やり直しもできません。
- [Enable Mobile User Security Service] : VPN を介したクライアントとの接続を開始します。イネーブルにすると、ASA への接続時に WSA によって使用されるパスワードを入力する必要があります。WSA が存在しない場合、ステータスは **disabled** になります。
- [Service Port] : サービスをイネーブルにする場合、サービスのどのポート番号を使用するかを指定します。ポートの範囲は 1 ~ 65535 で、管理システムにより WSA にプロビジョニングされた対応する値と一致させる必要があります。デフォルトは 11999 です。
- [Change Password] : WSA アクセスパスワードを変更できます。
- [WSA Access Password] : ASA と WSA の間の認証で必要となる共有シークレットパスワードを指定します。このパスワードは、管理システムにより WSA にプロビジョニングされた対応するパスワードと一致させる必要があります。
- [Confirm Password] : 指定したパスワードを再入力します。

- [Show WSA Sessions] : ASA に接続された WSA のセッション情報を表示できます。接続されている（または接続された）WSA のホスト IP アドレスおよび接続時間がダイアログボックスに返されます。

Add or Edit MUS Access Control

[設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [セキュアモビリティソリューション (Secure Mobility Solution)] の下の [MUS アクセス制御の追加または編集 (Add or Edit MUS Access Control)] ダイアログボックスで、AnyConnect クライアントの Mobile User Security (MUS) アクセスを設定します。

- [Interface Name] : ドロップダウン リストを使用して、追加または編集しているインターフェイス名を選択します。
- [IP Address] : IPv4 アドレスまたは IPv6 アドレスを入力できます。
- [Mask] : ドロップダウン リストを使用して、該当のマスクを選択します。

AnyConnect クライアントのカスタマイズとローカリゼーション

AnyConnect VPN クライアントの AnyConnect VPN モジュールをカスタマイズして、リモートユーザーに、会社のイメージを表示できます。[AnyConnect クライアントのカスタマイズ/ローカライズ (AnyConnect Client Customization/Localization)] のフィールドを使用すれば、次のタイプのカスタマイズされたファイルをインポートすることができます。

- **Resources** : AnyConnect クライアントの変更された GUI アイコン。
- **Binary** : AnyConnect クライアント インストーラに代わる実行可能ファイル。これには、GUI ファイルのほか、VPN クライアント プロファイル、スクリプト、その他のクライアント ファイルが含まれます。
- **Script** : AnyConnect クライアント が VPN 接続を確立する前または後に実行するスクリプト。
- **GUI Text and Messages** : AnyConnect クライアントが使用するタイトルとメッセージ。
- **Customized Installer** : クライアントのインストールを変更するトランスフォーム。
- **Localized Installer** : クライアントで使用される言語を変更するトランスフォーム。

各ダイアログでは次のアクションを実行できます。

- [インポート (Import)] をクリックすると、[AnyConnect クライアントのカスタマイズオブジェクトをインポート (Import AnyConnect Client Customization Objects)] ダイアログが起

動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。

- [エクスポート (Export)]をクリックすると、[AnyConnect クライアントのカスタマイズオブジェクトをエクスポート (Export Customization Objects)]ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。
- [Delete] をクリックすると、選択したオブジェクトが削除されます。



(注) この機能はマルチ コンテキスト モードではサポートされません。

AnyConnect クライアントのカスタマイズとローカリゼーション、リソース

インポートするカスタムコンポーネントのファイル名は、AnyConnect クライアント GUI で使用されるファイル名と一致している必要があります。これはオペレーティングシステムによって異なり、Mac および Linux では大文字と小文字が区別されます。たとえば、Windows クライアント用の企業ロゴを置き換えるには、独自の企業ロゴを `company_logo.png` としてインポートする必要があります。別のファイル名でインポートすると、AnyConnect クライアントインストーラはそのコンポーネントを変更しません。ただし、独自の実行ファイルを展開して GUI をカスタマイズする場合は、その実行ファイルから任意のファイル名のリソースファイルを呼び出すことができます。

イメージをソースファイルとして (たとえば、`company_logo.bmp`) インポートする場合、インポートしたイメージは、同じファイル名を使用して別のイメージを再インポートするまで、AnyConnect クライアントをカスタマイズします。たとえば、`company_logo.bmp` をカスタムイメージに置き換えて、このイメージを削除する場合、同じファイル名を使用して新しいイメージ (または元のシスコロゴイメージ) をインポートするまで、クライアントはこのイメージの表示を継続します。

AnyConnect クライアントのカスタマイズとローカリゼーション、バイナリとスクリプト

AnyConnect クライアントカスタマイゼーション/ローカリゼーション、バイナリ

Windows、Linux、または Mac (PowerPC または Intel ベース) コンピュータの場合、AnyConnect クライアント API を使用する独自のクライアントを展開できます。クライアントのバイナリファイルを置き換えることによって、AnyConnect クライアント GUI および AnyConnect クライアント CLI を置き換えます。

[Import] ダイアログのフィールドは次のとおりです。

- **Name** 置き換える AnyConnect クライアントファイルの名前を入力します。

- **Platform** ファイルを実行する OS プラットフォームを選択します。
- **Select a file** ファイル名は、インポートするファイルの名前と同じにする必要はありません。

AnyConnect クライアントカスタマイゼーション/ローカリゼーション、スクリプト

スクリプトの展開およびスクリプトの制限事項の詳細については、『AnyConnect VPN module of Cisco Secure Client Administrators Guide』を参照してください。

[Import] ダイアログのフィールドは次のとおりです。

- **Name** : スクリプトの名前を入力します。名前には正しい拡張子を指定してください。例 : myscript.bat.
- **Script Type** : スクリプトを実行するタイミングを選択します。

ASA でファイルをスクリプトとして識別できるように、AnyConnect クライアントによって、プレフィックス `scripts_` とプレフィックス `OnConnect` または `OnDisconnect` がユーザーのファイル名に追加されます。クライアントが接続すると、ASA は、リモートコンピュータ上の適切なターゲット ディレクトリにスクリプトをダウンロードします。その際、`scripts_` プレフィックスは削除され、`OnConnect` または `OnDisconnect` プレフィックスはそのまま残ります。たとえば、myscript.bat スクリプトをインポートした場合、ASA 上では、スクリプトは `scripts_OnConnect_myscript.bat` となります。リモートコンピュータ上では、スクリプトは `OnConnect_myscript.bat` となります。

スクリプトの実行の信頼性を確保するために、すべての ASA で同じスクリプトを展開するように設定します。スクリプトを修正または置換する場合は、旧バージョンと同じ名前を使用し、ユーザーが接続する可能性のあるすべての ASA に置換スクリプトを割り当てます。ユーザーが接続すると、新しいスクリプトにより同じ名前のスクリプトが上書きされます。

- **Platform** : ファイルを実行する OS プラットフォームを選択します。
- **Select a file** : ファイル名は、スクリプトに対して指定した名前と同じである必要はありません。

ASDM によってファイルがソース ファイルからインポートされ、[Name] に対して指定した新しい名前が作成されます。

AnyConnect クライアントのカスタマイズとローカリゼーション、GUI テキストとメッセージ

デフォルトの変換テーブルを編集するか、または新しいテーブルを作成して、AnyConnect クライアント GUI に表示されるテキストとメッセージを変更できます。このペインは、[Language Localization] ペインと同じ機能を持ちます。より高度な言語変換については、[Configuration] > [Remote Access VPN] > [Language Localization] に移動します。

上部ツールバーにある通常のボタンに加えて、このペインには[Add] ボタンと、追加のボタンを備えた [Template] エリアがあります。

Add : [Add] ボタンをクリックするとデフォルトの変換テーブルのコピーが開き、直接編集したり保存することができます。保存ファイルの言語を選択し、ファイル内のテキストの言語を後で編集することができます。

変換テーブルのメッセージをカスタマイズする場合、msgid は変更しないでください。msgstr 内のテキストを変更します。

テンプレートの言語を指定します。テンプレートはキャッシュメモリ内の変換テーブルになり、指定した名前が付きます。ブラウザの言語オプションと互換性のある短縮形を使用してください。たとえば、中国語のテーブルを作成するときに IE を使用している場合は、IE によって認識される zh という略語を使用します。

[Template] セクション

- テンプレート領域を展開してデフォルトの英語変換テーブルにアクセスするには、[Template] をクリックします。
- デフォルトの英語変換テーブルを表示し、必要に応じて保存するには、[View] をクリックします。
- デフォルトの英語変換テーブルのコピーを表示せずに保存するには、[Export] をクリックします。

AnyConnectクライアントのカスタマイズとローカリゼーション、カスタマイズされたインストーラ トランスフォーム

作成した独自のトランスフォームを、クライアントインストーラプログラムを使用して展開することによって、AnyConnect クライアント GUI を大幅にカスタマイズすることができます (Windows のみ)。トランスフォームを ASA にインポートすると、インストーラプログラムを使用して展開されます。

トランスフォームの適用先として選択できるのは Windows だけです。トランスフォームの詳細については、『Cisco Secure Client Administration Guide』を参照してください。

AnyConnectクライアントのカスタマイズとローカリゼーション、ローカライズされたインストーラ トランスフォーム

トランスフォームを使用して、クライアントインストーラプログラムに表示されるメッセージを翻訳できます。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これらのトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

AnyConnect クライアント カスタム属性

カスタム属性は AnyConnect クライアント に送信され、以下に示すような機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。これらのカスタム属性の設定については、『[Configure Secure Client Custom Attributes in an Internal Group Policy](#)』を参照してください。多数のさまざまな用途のカスタム属性を作成および設定します。

- **DSCPPreservationAllowed** : (DSCP の保存を有効化) このカスタム属性を設定すると、Windows または Mac のオペレーティング システム プラットフォームで DTLS 接続の Differentiated Services Code Point (DSCP) が制御されます。この属性を使用すると、デバイスは、遅延の影響を受けやすいトラフィックを優先順位付けし、優先順位付けされたトラフィックにマークを付けてアウトバウンド接続の質を改善することができます。詳細については、『[Cisco Secure Client Administration Guide](#)』の「*Enable DSCP Preservation*」セクションを参照してください。

値は True または False です。デフォルトでは、AnyConnect クライアント は DSCP の保存を実行します (True)。無効にするには、ヘッドエンドでカスタム属性値を false に設定し、接続を再初期化します。

- **DeferredUpdateAllowed** または **DeferredUpdateAllowed_ComplianceModule** : (ASA で更新の延期を有効化) これらのカスタム属性が設定されている場合に、クライアントの更新が利用可能になると、AnyConnect クライアント は更新を実行するか延期するかをユーザーに尋ねるダイアログを開きます。詳細については、『[Cisco Secure Client Administration Guide](#)』の「[Enable AnyConnect クライアント Deferred Upgrade](#)」または「[Configure Deferred Update on an ASA](#)」を参照してください。

値は True または False です。True の場合、更新の延期が有効になります。更新の延期が無効 (False) の場合、下記の設定は無視されます。

- **DeferredUpdateMinimumVersion_ComplianceModule** または **DeferredUpdateMinimumVersion** : 更新を延期できるようにするためにインストールする必要がある最小バージョンの AnyConnect クライアント。

値は x.x.x で、デフォルトは 0.0.0 です。

- **DeferredUpdateDismissTimeout** : 更新の延期を確認するダイアログが表示されてから、自動的に閉じるまでの秒数。更新の延期を確認するダイアログが表示される場合にのみ適用されます。

値は 0 - 300 秒です。デフォルトは 150 秒です。

- **DeferredUpdateDismissResponse** : DeferredUpdateDismissTimeout の発生時に実行するアクション。

値は defer (延期) または update (更新) です。デフォルトは update です。

- **dynamic-split-exclude-domains** <属性名><ドメインのリスト> または **dynamic-split-include-domains** <属性名><ドメインのリスト> : (ダイナミック スプリット トンネリングを有効化) このカスタム属性を作成することにより、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。dynamic-split-exclude-domains を追加することにより、VPN トンネルの外部のクライアントによるアクセスが必要なクラウドまたは Web サービスを入力できます。詳細については、『[Cisco Secure Client Administration Guide](#)』の「*About Dynamic Split Tunneling*」を参照してください。

値の属性名には、任意の名前を指定できます。たとえば、anyconnect-custom-data dynamic-split-exclude-domains excludedomains webex.com, ciscospark.com のようにします。

- **managementTunnelAllAllowed** : (管理 VPN トンネルを有効化) ユーザーが開始したネットワーク通信に影響しないように (管理 VPN トンネルは透過的であるため) スプリット 包含トンネリングの設定がデフォルトで必要です。

値は true または false です。この動作をオーバーライドする場合は、属性名と値の両方を true に設定します。そのように設定すると、両方の IP プロトコルの設定が tunnel-all、split-exclude、split-include、または bypass のいずれかの場合、AnyConnect クライアントは管理トンネルの接続に進みます。

- **UseLocalProfileAsAlternative** : Cisco Secure Firewall ASA で Cisco Secure Client プロファイル (旧名は AnyConnect) を設定せずに、アウトオブバンドで (SCCM、MDM、SecureX Cloud Management などを使用して) プロファイルを配布する場合は、*UseLocalProfileAsAlternative* カスタム属性を使用できます。このカスタム属性を設定すると、クライアントは設定とプリファレンスに (通常のデフォルトではなく) ローカル (ディスク上) の Cisco Secure Client プロファイルを使用します。詳細については、アドミニストレーションガイドの「[Predeploying Cisco Secure Client](#)」を参照してください。

ローカルプロファイルを使用したセッションの確立は、1) UseLocalProfileAsAlternative が有効に設定されている場合、および 2) ASA グループ ポリシー プロファイルが設定されていない場合にのみ発生します。このカスタム属性を設定し、ASA のグループポリシー構成から Cisco Secure Client プロファイルを元に戻したり削除したりしない場合、グループポリシーで構成された Cisco Secure Client プロファイルが維持され、カスタム属性の設定が無視される各接続で使用されます。

名前 : 無効/有効

値 : true/false

- **no-dhcp-server-route** : (パブリック DHCP サーバールートの設定) このカスタム属性により、Tunnel All Network が設定されている場合にローカル DHCP トラフィックがクリアテキストで流れるようになります。AnyConnect クライアントは、AnyConnect クライアントの接続時にローカル DHCP サーバーに特定のルートを追加し、ホストマシンの LAN アダプターに暗黙的なフィルタを適用して、DHCP トラフィックを除く当該ルートのすべてのトラフィックをブロックします。詳細については、『[Cisco Secure Client Administration Guide](#)』の「*Set Public DHCP Server Route*」セクションを参照してください。

値は true または false です。トンネル確立時のパブリック DHCP サーバー ルート作成を避けるために、no-dhcp-server-route カスタム属性が存在し、true に設定されている必要があります。

- **circumvent-host-filtering** : (サブネットの除外をサポートするように Linux を設定) [Tunnel Network List Below] がスプリットトンネリング用に設定されている場合はサブネットの除外をサポートするように、Linux を設定します。詳細については、[サブネットの除外をサポートするための Linux の設定 \(31 ページ\)](#) を参照してください。

値は true または false です。true に設定します。

- **tunnel-from-any-source** : (Linuxのみ) AnyConnect クライアントは、Split-Include または Split-Exclude トンネルモードの任意の送信元アドレスを持つパケットを許可します。VM インスタンスまたは Docker コンテナ内のネットワークアクセスを許可できます。



(注) VM/Docker で使用されるネットワークは、最初にトンネルから除外する必要があります。

- **perapp** : モバイルデバイス (Android または Apple iOS のみ) 上の特定のアプリケーションセットで VPN 接続が使用されます。詳細については、『*Cisco Secure Client Administration Guide*』の「Create Per App Custom Attributes」セクションを参照してください。

値を指定する際は、ポリシーツールから BASE64 形式をコピーしてここに貼り付けて、1 つ以上の値を追加します。

これらの機能の使用をさらに完全にするには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > メニューで、定義済みカスタム属性のほとんどを特定のグループ ポリシーに関連付ける必要があります。

IPsec VPN クライアント ソフトウェア



(注) VPN クライアントは耐用年数末期で、サポートが終了しています。VPN クライアントの設定については、ASA バージョン 9.2 に関する ASDM のマニュアルを参照してください。AnyConnect セキュア モビリティ クライアントにアップグレードすることを推奨します。

Zone Labs Integrity Server

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Zone Labs Integrity Server] パネルでは、Zone Labs Integrity Server をサポートするように ASA を設定できます。このサーバーは、プライベート ネットワークにアクセスするリモート クライアントでセキュリティ ポリシーを適用する目的で設計された Integrity System というシステムの一

部です。実質的には、ASAがファイアウォールサーバーに対するクライアントPCのプロキシとして機能し、IntegrityクライアントとIntegrityサーバー間で必要なすべてのIntegrity情報をリレーします。



(注) 現在のリリースのセキュリティアプライアンスでは同時に1台のIntegrityサーバーのみがサポートされていますが、ユーザーインターフェイスでは最大5台のIntegrityサーバーの設定がサポートされています。アクティブなサーバーに障害が発生した場合は、ASA上で別のIntegrityサーバーを設定して、クライアントVPNセッションを再確立してください。

- [Server IP address] : IntegrityサーバーのIPアドレスを入力します。ドット付き10進数を使用します。
- [Add] : 新しいサーバーIPアドレスをIntegrityサーバーのリストに追加します。このボタンは、Server IPアドレスフィールドにアドレスが入力されるとアクティブになります。
- [Delete] : 選択したサーバーをIntegrityサーバーのリストから削除します。
- [Move Up] : 選択したサーバーをIntegrityサーバーのリスト内で上に移動します。このボタンは、リストにサーバーが1台以上存在する場合にだけ使用できます。
- [Move Down] : 選択したサーバーをIntegrityサーバーのリスト内で下に移動します。このボタンは、リストにサーバーが1台以上存在する場合にだけ使用できます。
- [Server Port] : アクティブなIntegrityサーバーをリッスンするASAのポート番号を入力します。このフィールドは、Integrity Serverのリストにサーバーが少なくとも1台以上存在する場合にだけ使用できます。デフォルトポート番号は5054、範囲は10～10000です。このフィールドは、Integrity Serverリスト内にサーバーが存在する場合にだけ使用できます。
- [Interface] : アクティブなIntegrityサーバーと通信するASAインターフェイスを選択します。このインターフェイス名メニューは、Integrity Serverリスト内にサーバーが存在する場合にだけ使用できます。
- [Fail Timeout] : ASAがアクティブなIntegrityサーバーに到達できないことを宣言するまでの待機秒数を入力します。デフォルトは10で、範囲は、5～20です。
- [SSL Certificate Port] : SSL認証で使用するASAのポートを指定します。デフォルトのポートは80です。
- [Enable SSL Authentication] : ASAによるリモートクライアントのSSL証明書の認証をイネーブルにする場合にオンにします。デフォルトでは、クライアントSSL認証はディセーブルになっています。
- [Close connection on timeout] : タイムアウト時にASAとIntegrityサーバー間の接続を終了する場合にオンにします。デフォルトでは、接続が維持されます。
- [Apply] : 設定を実行しているASAにIntegrityサーバーの設定を適用します。
- [Reset] : まだ適用されていないIntegrityサーバーの設定の変更を削除します。

ISE ポリシーの適用

Cisco Identity Services Engine (ISE) は、セキュリティポリシー管理および制御プラットフォームです。有線、ワイヤレス、VPN 接続のアクセス制御とセキュリティコンプライアンスを自動化し、シンプルにします。Cisco ISE は主に、Cisco TrustSec と連携してセキュアアクセスとゲストアクセスを提供し、個人所有デバイス持ち込み (BYOD) イニシアティブをサポートし、使用ポリシーを適用するために使用されます。

ISE Change of Authorization (CoA) 機能は、認証、認可、およびアカウントिंग (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を変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インラインポスチャ実施ポイント (IPEP) は、ASA 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。

ISE ポリシーの実施は、次の VPN クライアントでサポートされています。

- IPSec
- AnyConnect クライアント
- L2TP/IPSec

システムフローは次のとおりです。

1. エンドユーザーが VPN 接続を要求します。
2. ASA は、ISE に対してユーザーを認証し、ネットワークへの限定アクセスを提供するユーザー ACL を受け取ります。
3. アカウント開始メッセージが ISE に送信され、セッションが登録されます。
4. ポスチャアセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。
5. ISE が CoA の「ポリシープッシュ」を介して ASA にポリシーの更新を送信します。これにより、ネットワークアクセス権限を高める新しいユーザー ACL が識別されます。



(注) 後続の CoA 更新を介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

ISE 許可変更の設定

ISE 認可変更を設定するには、ISE RADIUS サーバーを含むサーバーグループを作成し、リモートアクセス VPN 設定プロファイル (トンネル) でそのサーバーグループを使用します。

手順

ステップ 1 ISE サーバーの RADIUS AAA サーバー グループを設定します。

次の手順は、最小限の設定を示しています。必要に応じて、グループの他の設定を調整できます。大部分の設定には、ほとんどのネットワークに適したデフォルト設定があります。RADIUS AAA サーバー グループの設定の詳細については、一般的なコンフィギュレーションガイドを参照してください。

- a) **[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups]** を選択します。
- b) **[AAA Server Group]** 領域で、**[Add]** をクリックします。
- c) **[Server Group]** フィールドにグループの名前を入力します。
- d) **[Protocol]** ドロップダウン リストから **RADIUS サーバー タイプ** を選択します。
- e) **[Enable interim accounting update]** と **[Update Interval]** を選択し、**RADIUS 中間アカウントティング更新メッセージ** が定期的に生成されるようにします。

ISE は、ASA などの NAS デバイスから受信するアカウントティングレコードに基づいて、アクティブセッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウントティングメッセージまたはポスチャトランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブセッションについて ISE に定期的に中間アカウントティング更新メッセージを送信するように、グループを設定します。

これらの更新を送信する間隔を時間単位で変更できます。デフォルトは 24 時間で、指定できる範囲は 1 ~ 120 です。

- f) **[Enable dynamic authorization]** を選択します。

このオプションは、AAA サーバー グループの RADIUS の動的認可（ISE 許可変更、CoA）サービスをイネーブルにします。VPN トンネルでサーバー グループを使用すると、対応する RADIUS サーバー グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。別のポートを使用するように ISE サーバーが設定されていない限り、ポート（1700）を変更しないでください。有効な範囲は 1024 ~ 65535 です。

- g) 認証に ISE を使用しない場合は、**[Use authorization only mode]** を選択します。

このオプションは、サーバー グループを認可に使用するとき、RADIUS アクセス要求メッセージが、AAA サーバー用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。RADIUS サーバーの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバー グループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウントティングにこのサーバー グループを使用する可能性があるからです。

- h) **[OK]** をクリックして、サーバー グループを保存します。

- i) サーバー グループを選択したら、[Servers in the Selected Group] リストで [Add] をクリックし、ISE RADIUS サーバーをグループに追加します。

キー属性を以下に示します。必要に応じて、他の設定用にデフォルトを調整できます。

- [Interface Name] : ISE サーバーに到達するためのインターフェイス。
- [Server Name or IP Address] : ISE サーバーのホスト名または IP アドレス。
- (任意) [Server Secret Key] : 接続を暗号化するキー。キーを設定しないと、接続は暗号化されません (プレーンテキスト)。このキーは 127 文字までの英数字から構成され、大文字と小文字の区別があり、RADIUS サーバー上のキーと同じ値になります。

- j) [OK] をクリックして、サーバーをグループに追加します。
サーバー グループに別の ISE サーバーを追加します。

ステップ 2 リモートアクセス VPN で ISE サーバー グループを使用するために、設定プロファイルを更新します。

以下の手順は、ISE 関連の設定オプションにのみ該当します。機能的なリモートアクセス VPN を作成するには、その他のオプションも設定する必要があります。リモートアクセス VPN の実装については、このマニュアルの他の箇所の説明に従ってください。

- a) [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] [AnyConnect クライアント接続プロファイル (Connection Profiles)] を選択します。
- b) [Connection Profiles] テーブルで、プロファイルを追加または編集します。
- c) [Basic] ページで、認証方式を設定します。
 - 認証に ISE サーバーを使用する場合は、[Authentication] > [Method] に対して [AAA] を選択し、次に ISE AAA サーバー グループを選択します。
 - 許可用にのみ ISE サーバー グループを設定する場合は、別の認証方式 ([Certificate] など) を選択します。
- d) [Advanced] > [Authorization] ページで、[Authorization Server Group] に対して ISE サーバー グループを選択します。
- e) [Advanced] > [Accounting] ページで、ISE サーバー グループを選択します。
- f) [OK] をクリックして変更を保存します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。