一般的な VPN 設定

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 [Maximum AnyConnect 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 [適用（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 （40 ページ）を参照してください。

手順

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

a) [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] の [Access Interfaces] セクションに移動します。

b) [Interface] テーブルの AnyConnect 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) [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] 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 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 グループ名、サーバ、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 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 グループとして使用するサーバを選択します。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 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、スマート トンネル、およびポート転送において、ユーザ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）。これは、ASA 5500-X シリーズデバイスのデフォルトバイアスです。
- [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 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。

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 サーバに格納されているユーザ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 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 サーバまたはLDAP サーバ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：DNS および WINS サーバ、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]）。
- ユーザ認証サーバと内部認証サーバ（[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、クライアントレス SSL 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。AnyConnect セキュア モビリティ クライアントおよび 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 クライアントの内部グループ ポリシー （19 ページ）
- クライアントレス SSL VPN の内部グループ ポリシー （51 ページ）：これは、ブラウザ ベースの VPN アクセスとも呼ばれます。ASA のポータル ページに正常にログインすると、リモート ユーザは Web ページに表示されるリンクから企業ネットワークとアプリケーションにアクセスできます。リモート ユーザと企業ネットワーク間のデータ トラフィックは、SSL トンネルを通過する際に保護されます。
- サイト間内部グループ ポリシー （56 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 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 サーバのユーザ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 サーバはクエリーをユーザ 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 サーバ上のユーザ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と同じRADIUS サーバに存在する場合、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を設定し、それらの属性のサブセットから個々のユーザに対する特定の許可を割り当てる必要があります。外部サーバを設定するには、「認可および認証用の外部サーバ」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 グループを一覧表示します。
- [New]：新しい RADIUS サーバ グループまたは新しい LDAP サーバ 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 グループ ポリシーのパスワードを指定します。

AAA サーバ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、LDAP サーバなどの AAA サーバで有効です。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。

- AnyConnect VPN クライアント
- IPsec VPN クライアント
- IPsec IKEv2 クライアント
- クライアントレス SSL VPN

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（Cisco ACS など）は、認証要求を別の認証サーバ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 でのパスワードのサポート

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

- ユーザ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 サーバからのパスワード期限切れの通知を無視し、ユーザ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 サーバは、AD にプロキシする RADIUS サーバ、または LDAP サーバ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、ユーザが RADIUS サーバ 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 ユーザの場合は、/n タグを使用します。
  - AnyConnect クライアント ユーザの場合は、
 タグを使用します。

- [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 Client]：Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアント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 セキュア モビリティ 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 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。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 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（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）。
- 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、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、サーバ属性

[Group Policy] > [Servers] ウィンドウで、DNS サーバ、WINS サーバおよび DNS スコープを設定します。DNS および WINS サーバはフル トンネル クライアント（IPsec、AnyConnect、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 [適用（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 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 アクセスから除外するサーバの名前と IP アドレスを一覧表示します。プロキシサーバ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を設定し、一時的な状態に基づいてユーザがその中からプロキシサーバ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
  - [Allow Proxy Lockdown for Client System]：この機能をイネーブルにすると、AnyConnect VPN セッションの間、Microsoft Internet Explorer の [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 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 バージョン 4.7.03052 以降が必要です。

AnyConnect 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、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に対する使用などがあります。
- [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 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、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアル スタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコル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が 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 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 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 デバイスを通し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実行していないときでも、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。

- [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 DART：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がキャプチャされ、.zip ファイルがデスクトップに作成されます。

  - AnyConnect 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 SBL：Start Before Logon（SBL）では、Windows のログイン ダイアログ ボックスが表示される前に AnyConnect を開始することにより、ユーザが Windows にログインする前に VPN 接続を介してユーザを企業インフラに強制的に接続します。

  - AnyConnect 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 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 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 モジュールは AnyConnect バージョン 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 に統合され、これにより AnyConnect 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 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 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 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 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 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） 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 リリースが必要です。

- [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。[Add] をクリックして [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 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 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 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 ルールを評価するように AnyConnect 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 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 Names] フィールドに、トンネルを介して AnyConnect 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。

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。

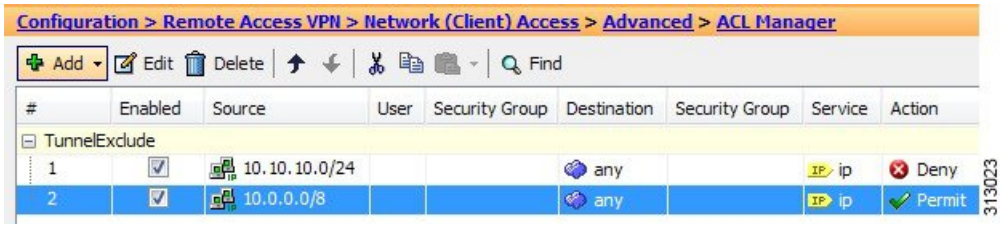
[Inherit] チェックボックスをオフにした場合は、次のいずれかのポリシー オプションを選択できます。

- [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。



（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、一般的操作用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 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect 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 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。[AnyConnect Custom Attribute Names] 画面の [Value] 部分で、カンマ文字でドメインを区切るカンマ区切り値（CSV）形式を使用し

てこれらのドメインを定義します。AnyConnect は、区切り文字を除いて最初の 5000 文字のみを考慮します（約 300 個の通常のサイズのドメイン名）。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、実行されます。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 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 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect 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 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。[AnyConnect Custom Attribute Names] 画面の [Value] 部分で、カンマ文字でドメインを区切るカンマ区切り値（CSV）形式を使用してこれらのドメインを定義します。AnyConnect は、区切り文字を除いて最初の 5000 文字のみを考慮します（約 300 個の通常のサイズのドメイン名）。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、**[Advanced] > [AnyConnect Client] > [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 インクルード 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 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 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect 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 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。[AnyConnect Custom Attribute Names] 画面の [Value] 部分で、カンマ文字でドメインを区切るカンマ区切り値（CSV）形式を使用してこれらのドメインを定義します。AnyConnect は、区切り文字を除いて最初の 5000 文字のみを考慮します（約 300 個の通常のサイズのドメイン名）。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、**[Advanced] > [AnyConnect Client] > [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 接続が確立されるときだけでなく、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 AnyConnect Secure Mobility 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、**[Configuration]** > **[Remote Access]** > **[Network (Client) Access]** > **[AnyConnect Connection Profiles]** > **[Add/Edit]** に移動し、[Authentication] の下の [Method] ドロップダウン メニューから選択して [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 カスタム属性 （126 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 （108 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、**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Advanced]** > **[AnyConnect 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、**[Advanced]** > **[AnyConnect Client]** > **[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

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] 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 ユーザの接続時間が短縮されます。

  （注） [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に対する使用などがあります。
- [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、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアル スタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコル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 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 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 デバイスを通し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実行していないときでも、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。

- [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 DART：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がキャプチャされ、.zip ファイルがデスクトップに作成されます。
  - AnyConnect 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 SBL：Start Before Logon（SBL）では、Windows のログイン ダイアログ ボックスが表示される前に AnyConnect を開始することにより、ユーザが Windows にログインする前に VPN 接続を介してユーザを企業インフラに強制的に接続します。
  - AnyConnect 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 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 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 に統合され、これにより AnyConnect 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 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 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 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 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 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） 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 リリースが必要です。

- [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。[Add] をクリックして [Select AnyConnect Client Profiles] ウィンドウを起動すると、グループ ポリシー用に以前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 ログイン設定

内部グループ ポリシーの **Advanced > AnyConnect Client > Login Setting** ペインでは、リモート ユーザに 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 [Advanced] > [AnyConnect Client] > [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は、ルールを修正できません。どちらのユーザの場合も、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、ユーザが Active Directory（AD）サーバで認証されると、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。

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 （36 ページ）
- VPN のテザー デバイス サポートの設定 （39 ページ）

ファイアウォールの動作に関する注意事項

ここに記載したのは、AnyConnect クライアントではファイアウォールがどのように使用されるかについての注意事項です。

- 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 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 クライアントへプッシュされても、ユーザがカスタムの拒否ルールを作成していれば、AnyConnect 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 ユーザは、VPN 接続の確立にかなりの時間を要する場合があります。
- Mac コンピュータの場合、AnyConnect クライアントでは、ASA で適用されたの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双方で許可された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タイプのトラフィックであっても、サードパーティ ファイアウォールによってブロックされれば、そのトラフィックはクライアントでもブロックされます。

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。

- 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。
- ホスト スキャン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	宛先ポート	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_Client_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_Client_Local_Print の ACL ルール

説明	Permission	インターフェイス	プロトコル	送信元ポート	Destination Address	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
LPD	許可	パブリック	TCP	デフォルト	いずれか（Any）	515

説明	Permission	インターフェイス	プロトコル	送信元ポート	Destination Address	宛先ポート
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　[Advanced] > [AnyConnect Client] > [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 を実行してい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 [Advanced] > [AnyConnect Client] > [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 SSL VPN クライアント間の接続のみに適用されます。DPD はパディングを許可しない標準の実装に基づいているため IPsec を使用できず、クライアントレス SSL VPN がサポートされません。
- 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。

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] の順に移動し、目的のグループ ポリシーを追加（[Add]）または編集（[Edit]）し、[Advanced] > [AnyConnect Client] > [Dead Peer Detection] ペインを開きます。
- または特定のユーザ ポリシーに到達するには、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] に移動し、目的のユーザ アカウントを追加（[Add]）または編集（[Edit]）し、[VPN Policy] > [AnyConnect Client] > [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。値 300 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 カスタマイズ

内部グループ ポリシーの [Advanced] > [AnyConnect Client] > [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。

- [Portal Customization]：[AnyConnect Client/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。クライアントレス ユーザには、認証の成功後すぐにこのページが表示されます。AnyConnect は、VPN 接続が正常に確立されると、この URL に対してデフォルトの Web ブラウザを起動します。

（注） AnyConnect 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 クライアントによって無視されます。

- [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 [Advanced] > [AnyConnect Client] > [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 リリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。

カスタム属性は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] および [AnyConnect 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 **[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Group Policies]** > **[Add/Edit]** > **[Advanced]** > **[AnyConnect Client]** > **[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。

a) [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。

b) [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 カスタム属性オプションについては、AnyConnect カスタム属性（126 ページ）を参照してください。

c) [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。

a) [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。

b) [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用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。

c) [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 サーバを指定できます。
  - [Server Configuration]：IPsec バックアップ サーバとして使用するサーバ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もありますが、この方法を使用すれば、ユーザ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、一部のユーザがファイアウォールをサポートしており、他のユーザ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 ポリシーと相関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。

内部グループ ポリシー、IPsec（IKEv1）のハードウェア クライアント属性

[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] > [Hardware Client] ダイアログボックスで、Easy VPN Remote クライアントに送信されるグループ ポリシー属性を設定します。ASA における Easy VPN のサポートの詳細については、Easy VPNの章を参照してください。

（注） VPN 3002 ハードウェア 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。

- [Inherit]：（複数インスタンス）対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。これは、このダイアログボックスの属性すべてのデフォルト設定になります。
- [Require Interactive Client Authentication]：インタラクティブ クライアント認証の要求をイネーブルまたはディセーブルにします。このパラメータはデフォルトではディセーブルになっています。

  ディセーブルにすると、ハードウェア クライアントに保存されているクレデンシャルが認証に使用されます。クレデンシャルが保存されていない場合は、ハードウェア クライアントが手動で認証します。保存されているクレデンシャルまたは入力されたクレデンシャルが有効な場合は、トンネルが確立されます。

  このオプションをイネーブルにすると、クライアントにユーザ名とパスワードが保存されているかどうかに関係なく、トンネルが開始されるたびにハードウェア クライアントに対して手動でユーザ名とパスワードを認証するように要求することによって、セキュリティが強化されます。入力したクレデンシャルが有効な場合は、トンネルが確立されます。

  セキュア ユニット認証では、ハードウェア クライアントが使用する接続プロファイルに対して認証サーバ グループが設定されている必要があります。プライマリ ASA でセキュア ユニット認証が必要な場合は、どのバックアップ サーバにもセキュア ユニット認証を設定する必要があります。

（注） この機能をイネーブルにした場合に VPN トンネルを確立するには、ユーザがユーザ名とパスワードを入力する必要があります。

- [Require Individual User Authentication]：個別のユーザ認証の要求をイネーブルまたはディセーブルにします。個別ユーザ認証は、VPN 3002 のプライベート ネットワークの許可されないユーザが中央サイトにアクセスできないように保護します。このパラメータはデフォルトではディセーブルになっています。

  個別ユーザ認証をイネーブルにした場合は、トンネルがすでに存在していても、ハードウェア クライアントを介して接続する各ユーザは、ASA の背後にあるネットワークにアクセスするために、Web ブラウザを開いて手動で有効なユーザ名とパスワードを入力する必要があります。

  認証を行うには、ブラウザの [Location] フィールドまたは [Address] フィールドに、ハードウェア クライアントのプライベート インターフェイスの IP アドレスを入力する必要があります。ブラウザに、ハードウェア クライアントのログイン ダイアログボックスが表示されます。認証するには、[Connect/Login Status] をクリックします。ASA の背後のリモート ネットワークにデフォルト ホームページがある場合、または、ASA の背後のリモート ネットワーク上にある Web サイトをブラウザで開く場合、ハードウェア クライアントは、ユーザ ログイン用の適切なページをブラウザで開きます。正常にログインすると、元々入力していたページがブラウザに表示されます。

  ユーザ認証がイネーブルになっている場合は、コマンドライン インターフェイスを使用してログインできません。ブラウザを使用する必要があります。ASA の背後のネットワーク上にある Web ベースではないリソース（電子メールなど）にアクセスを試みる場合は、ブラウザを使用して認証を行うまで、接続に失敗します。

  バナーを表示するには、個々のユーザ認証をイネーブルにする必要があります。1 人のユーザは、同時に最大 4 セッションのログインを実行できます。

  プライマリ ASA でユーザ認証が必要な場合は、どのバックアップ サーバにもユーザ認証を設定する必要があります。

- [User Authentication Idle Timeout]：ユーザのタイムアウト期間を設定します。セキュリティ アプライアンスは、この期間にユーザ トラフィックを受信しないと、接続を終了します。タイムアウト期間として、特定の分数または無期限を指定できます。

  - [Unlimited]：接続がタイムアウトにならないように指定します。 このオプションは、デフォルト グループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
  - [Minutes]：タイムアウト期間を分単位で指定します。 1 ～ 35791394 の整数を使用します。デフォルト値は Unlimited です。

  show uauth コマンドへの応答で示されるアイドル タイムアウトは、常に Cisco Easy VPN リモート デバイスのトンネルを認証したユーザのアイドル タイムアウト値になります。

- [Cisco IP Phone Bypass]：Cisco IP Phone にインタラクティブ個別ユーザ認証プロセスをバイパスさせます（イネーブルな場合）。デフォルトでは、Cisco IP Phone Bypass はディセーブルになっています。

  IP Phone 接続にネットワーク拡張モードを使用するように、ハードウェア クライアントを設定する必要があります。

- [LEAP Bypass]：[Require Individual User Authentication] がイネーブルの場合にのみ適用されます。シスコの無線デバイスからの LEAP パケットに、個々のユーザ認証プロセスをバイパスさせます。LEAP Bypass は、デフォルトでディセーブルになっています。

  ハードウェア クライアントの後ろにいる LEAP ユーザには、面倒な問題があります。トンネルで中央サイト デバイスの後ろにある RADIUS サーバにクレデンシャルを送信することができないため、LEAP 認証をネゴシエートできません。トンネル経由でクレデンシャルを送信できない理由は、無線ネットワークで認証されていないためです。この問題を解決するために、LEAP バイパスは、個別のユーザ認証の前に LEAP パケット（LEAP パケットだけ）をトンネルで転送し、RADIUS サーバへの無線接続を認証できるようにします。これによって、ユーザは、個別のユーザ認証に進むことができます。

  LEAP Bypass は、次の条件下で適切に機能します。

  - [Require Interactive Client Authentication] がディセーブルになっている。インタラクティブ ユニット認証がイネーブルの場合、トンネルを使用して LEAP デバイスが接続できるようになる前に、非 LEAP（有線）デバイスがハードウェア クライアントを認証する必要があります。
  - [Require Individual User Authentication] がイネーブルになっている。イネーブルになっていないと、LEAP Bypass が適用されません。
  - 無線環境のアクセス ポイントが、Cisco Discovery Protocol（CDP）を実行している Cisco Aironet Access Point であること。PC の NIC カードは、他のブランドの製品でもかまいません。

- [Allow Network Extension Mode]：このグループのハードウェア クライアントによるネットワーク拡張モードの使用を決定します。このパラメータはデフォルトではディセーブルになっています。ネットワーク拡張モードがディセーブルになっている場合、ハードウェア クライアントはポート アドレス変換モードで ASA に接続する必要があります。

  Call Manager は実際の IP アドレスでだけ通信できるため、ハードウェア クライアントが IP Phone 接続をサポートするには、ネットワーク拡張モードが必要です。

（注） このグループのハードウェア クライアントを同様に設定する必要があります。ネットワーク拡張モードを使用するようにハードウェア クライアントが設定されており、接続先の ASA でネットワーク拡張モードがディセーブルになっている場合、ハードウェア クライアントは 4 秒ごとに接続を試行し、すべての試行が拒否されます。このような場合、ハードウェア クライアントは、接続先の ASA に不要な処理負荷をかけることになります。多数のハードウェア クライアントがこのように誤設定されていると、セキュリティ アプライアンスのサービス提供能力が損なわれます。

クライアントレス SSL VPN の内部グループ ポリシー

内部グループ ポリシー、クライアントレス SSL VPN 一般属性

[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit] > [General]

[Add or Edit Group Policy] ダイアログボックスでは、追加または変更するグループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、サーバを指定できます。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。

[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。

- [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に対して表示するバナー テキストを指定します。全体的なバナーの長さは最大 4000 文字です。デフォルト値はありません。

  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。

  - クライアントレス ユーザの場合は 、
 タグを使用します。

- [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 Client]：Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアント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]：AnyConnect セキュア モビリティ 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 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。

- [Web ACL]：（Clientless SSL VPN 専用）トラフィックをフィルタリングする場合は、ドロップダウン リストからアクセス コントロール リスト（ACL）を選択します。選択する前に ACL を表示、変更、追加、または削除する場合は、リストの横にある [Manage] をクリックします。
- [Access Hours]：このユーザ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。時間範囲オブジェクトを表示または追加するには、リストの横にある [Manage] をクリックします。
- [Simultaneous Logins]：このユーザ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 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（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（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）。
- 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 Connection Time Alert Interval：ユーザ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。
- Idle Timeout Alert Interval：アイドル タイムアウトに達すると、ユーザにメッセージが表示されます。

  [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。
- 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、クライアントレス SSL VPN アクセス ポータル

[Portal] 属性により、クライアントレス SSL VPN 接続を確立するこのグループ ポリシーのメンバのポータル ページに表示されるコンテンツが決まります。このペインでは、ブックマーク リストと URL エントリ、ファイル サーバ アクセス、ポート転送とスマート トンネル、ActiveX リレー、および HTTP の設定をイネーブルにできます。

- [Bookmark List]：あらかじめ設定されたブックマーク リストを選択するか、または [Manage] をクリックして新しいリストを作成します。ブックマークはリンクとして表示され、ユーザはこのリンクを使用してポータル ページから移動できます。
- [URL Entry]：リモート ユーザが URL をポータル URL フィールドに直接入力できるようにする場合にイネーブルにします。
- [File Access Control]：共通インターネット ファイル システム（CIFS）ファイルの「非表示共有」の表示状態を制御します。非表示共有は、共有名の末尾のドル記号（$）で識別されます。たとえば、ドライブ C は C$ として共有されます。非表示共有では、共有フォルダは表示されず、ユーザはこれらの非表示リソースを参照またはアクセスすることを禁止されます。
  - [File Server Entry]：リモート ユーザがファイル サーバの名前を入力できるようにする場合にイネーブルにします。
  - [File Server Browsing]：リモート ユーザが使用可能なファイル サーバを参照できるようにする場合にイネーブルにします。
  - [Hidden Share Access]：共有フォルダを非表示にする場合にイネーブルにします。
- [Port Forwarding Control]：Java Applet によるクライアントレス SSL VPN 接続により、ユーザが TCP ベースのアプリケーションにアクセスできるようにします。
  - [Port Forwarding List]：このグループ ポリシーに関連付ける事前設定済み TCP アプリケーションのリストを選択します。新しいリストを作成したり、既存のリストを編集したりするには、[Manage] をクリックします。
  - [Auto Applet Download]：ユーザが始めてログインするときに実行される、Java Applet の自動インストールおよび起動をイネーブルにします。
  - [Applet Name]：[Applet] ダイアログボックスのタイトルバーの名前を、指定する名前に変更します。デフォルトの名前は [Application Access] です。
- [Smart Tunnel]：スマート トンネルで使用されるクライアントレス（ブラウザベース）SSL VPN セッションにおいて、ASA がパスウェイ、セキュリティ アプライアンスがプロキシ サーバである場合に、スマート トンネルのオプションを指定します。
  - [Smart Tunnel Policy]：ネットワーク リストから選択し、いずれか 1 つのトンネル オプションを指定します（[use smart tunnel for the specified network]、[do not use smart tunnel for the specified network]、または [use tunnel for all network traffic]）。スマート トンネル ネットワークをグループ ポリシーまたはユーザ名に割り当てると、そのグループ ポリシーまたはユーザ名にセッションが関連付けられているすべてのユーザの場合

にスマート トンネル アクセスがイネーブルになりますが、リストで指定されているアプリケーションへのスマート トンネル アクセスは制限されます。スマート トンネル リストを表示、追加、変更、または削除するには、[Manage] をクリックします。

- [Smart Tunnel Application]：ドロップダウン リストから選択し、エンド ステーションにインストールされている TCP ベースのアプリケーション Winsock 2 をイントラネット上のサーバに接続します。スマート トンネル アプリケーションを表示、追加、変更、または削除するには、[Manage] をクリックします。
- [Smart Tunnel all Applications]：すべてのアプリケーションをトンネリングするには、このチェックボックスをオンにします。ネットワーク リストから選択したり、エンド ユーザが外部アプリケーション用に起動する可能性がある実行ファイルを認識したりすることなく、すべてのアプリケーションがトンネリングされます。
- [Auto Start]：ユーザのログイン時に、スマート トンネル アクセスを自動的に開始するには、このチェックボックスをオンにします。ユーザのログイン時にスマート トンネル アクセスを開始するこのオプションは Windows だけに適用されます。ユーザのログイン時にスマート トンネル アクセスをイネーブルにして、ユーザに手動で開始するように要求する場合はこのチェックボックスをオフにします。ユーザは、[Clientless SSL VPN Portal] ページの [Application Access] > [Start Smart Tunnels] ボタンを使用してアクセスを開始できます。
- [Auto Sign-on Server List]：ユーザがサーバへのスマート トンネル接続を確立するときにユーザ クレデンシャルを再発行する場合、ドロップダウン リストからリスト名を選択します。各スマート トンネル自動サインオン リストのエントリは、ユーザ クレデンシャルのサブミッションを自動化するサーバを示します。スマート トンネル自動サインオン リストを表示、追加、変更、または削除するには、[Manage] ボタンをクリックします。
- [Windows Domain Name (Optional)]：共通命名規則（domain\username）が認証に必要な場合、自動サインオン二次ユーザ名に追加する Windows のドメインを指定します。たとえば、ユーザ名 qu_team の認証を行う場合、CISCO と入力して CISCO\qa_team を指定します。自動サインオン サーバ リストで関連するエントリを設定する場合、[Use Windows domain name with user name] オプションもオンにする必要があります。

- [ActiveX Relay]：クライアントレス ユーザが Microsoft Office アプリケーションをブラウザから起動できるようにします。アプリケーションは、セッションを使用して Microsoft Office ドキュメントのダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。

その他のオプション：

- [HTTP Proxy]：クライアントへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングを回避できます。転送プロキシは、ブラウザの古いプロキシ設定を自動的に修正し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、

JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。

- [Auto Start (HTTP Proxy)]：ユーザのログイン時に HTTP プロキシを自動的にイネーブルにする場合にオンにします。ユーザ ログイン時にスマート トンネル アクセスをイネーブルにして、ユーザに手動で開始するように要求する場合はオフにします。
- [HTTP Compression]：クライアントレス SSL VPN セッションでの HTTP データの圧縮をイネーブルにします。

内部グループ ポリシーの設定、クライアントレス SSL VPN のポータルのカスタマイズ

グループ ポリシーのカスタマイゼーションを設定するには、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ます。表示する URL を設定することもできます。

クライアントレス SSL VPN アクセス接続にアクセス ポータルをカスタマイズするための手順は、ネットワーク アクセス クライアント接続と同じです。内部グループ ポリシー、クライアントレス ポータルの AnyConnect カスタマイズ （41 ページ）を参照してください。

内部グループ ポリシー、クライアントレス SSL VPN のログイン設定

リモート ユーザに 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 ページに移動するように ASA を設定できます。内部グループ ポリシー、AnyConnect ログイン設定 （34 ページ）を参照してください。

内部グループ ポリシー、クライアントレス SSL VPN アクセス用のシングル サインオン サーバと自動サインオン サーバ

シングル サインオン サーバと自動サインオン サーバを設定するには、内部グループ ポリシー、クライアントレス SSL VPN アクセス ポータル （54 ページ）を参照してください。

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、またはクライアントレス SSL VPN 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 Client]：Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアント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]：AnyConnect セキュア モビリティ 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 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]：（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。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（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）。

- 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 ユーザの VPN ポリシー属性の設定

この手順では、既存のユーザを編集する方法について説明します。ユーザを追加するには、[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 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 ユーザのグループ ポリシーを指定します。ユーザ 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/TLS を利用する VPN）クライアントレス SSL VPN では、Web ブラウザを使用して VPN コンセントレータへのセキュアなリモート アクセス トンネルを確立し、ソフトウェア クライアントもハードウェア クライアントも必要としません。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 クライアントは、Cisco AnyConnect Client アプリケーションのダウンロード後にユーザが接続できるようにします。ユーザは、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 セキュア モビリティ 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 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。
- 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。

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、ユーザが制限されます。一

致していない場合、ASA はユーザ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ます（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 アクセスを禁止します。

（注） 最大値を設定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、このパラメータで出アイドル 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 [Clientless SSL VPN] または [AnyConnect Client] 設定を設定します。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、Cisco AnyConnect VPN クライアント、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 接続プロファイル、メイン ペイン

AnyConnect 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 テーブルの AnyConnect 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 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 Anyconnect 機能が含まれていま

す。クライアント サービスをディセーブルにしても、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 （63 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 （63 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 接続プロファイルおよびクライアントレス接続プロファイル用です。Alway-on IPsec/IKEv2 などの特定の AnyConnect 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 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。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles]

[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [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 接続プロファイル、基本属性

AnyConnect VPN 接続の基本属性を設定するには、[AnyConnect Connection Profiles] セクションで [Add] または [Edit] を選択します。[Add/Edit AnyConnect Connection Profile] > [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]：認識の方法を、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 SSL と IKEv2 クライアントプロトコルでセッションごとに複数の証明書を検証できます。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、または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。
- [Client Address Assignment]：使用する DHCP サーバ、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 サーバ属性
- クライアントレス SSL VPN 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 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 日前にユーザへの通知を開始し、以後、ユーザ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。

- **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect 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 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、IKEv1 または IKEv2）を開き、[Advanced] > [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名の一覧を表示します。

- ASA 上のアドレス プールを削除するには、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 （68 ページ）
接続プロファイル、アドレス プール （69 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 （69 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 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 グループの割り当てを管理します。

- [Add or Edit]：[Assign Authentication Server Group to Interfac]e 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グループを指定するとともに、選択したサーバ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 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]：抽出したユーザ名はエンド ユーザに表示されません。
  - [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。

属性	定義
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
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 ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。

- [Primary Field]：ユーザ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。証明書のユーザ名の事前入力と 2 次認証を組み合わせて使用できます。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 次ユーザ名/パスワード認証処理に 2 つ目のユーザ名を使用するよう強制されます。

（注） 証明書のセカンダリ ユーザ名とともに 2 次認証サーバ 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 グループを指定します。
  - [Server Group]：セカンダリ サーバ AAA グループとして使用する認証サーバ グループを選択します。デフォルトは none です。SDI サーバ グループはセカンダリ サーバ 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 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かセカンダリ属性サーバかを選択します。

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

- [Session Username Server]：プライマリ セッション ユーザ名サーバかセカンダリ セッション ユーザ名サーバかを指定します。

- [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 グループの割り当てを管理します。
  - [Add or Edit]：[Assign Authentication Server Group to Interfac]e 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グループを指定するとともに、選択したサーバ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 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名を VPN ユーザ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、Cisco Secure Desktop のホストスキャン データを使用して、2 次認証のユーザ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 ユーザ名/パスワード認証または認可に証明書のユーザ名事前入力機能でこのユーザ名を使用するには、ユーザ名事前入力およびセカンダリ ユーザ名事前入力も設定する必要があります。
  - [Primary Field]：ユーザ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）。
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 ID）。
UPN	User Principal Name（ユーザ 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 接続プロファイル、認可属性

AnyConnect 接続プロファイルの [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グループ、および選択したサーバ 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、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 グループを指定します。
  - [Server Group]：使用する認可サーバ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。AAA サーバの設定については、クライアントレス SSL VPN 接続プロファイル、認証、サーバグループの追加 （84 ページ）を参照してください。
  - [Users must exist in the authorization database to connect]：ユーザ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 グループの割り当てを管理します。
  - [Add or Edit]：[Assign Authentication Server Group to Interfac]e 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グループを指定するとともに、選択したサーバ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 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接続プロファイル、認可、ユーザ名を選択するためのスクリプトの内容の追加

AnyConnect 接続プロファイルの [Authorization] ペインで [use a script to select username] を選択し、[Add] または [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名事前入力でクライアント証明書のユーザ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「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.l
```

1 つのユーザ名として使用する 2 つの DN フィールド、ユーザ名（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 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 ID
cert.serialnumber	証明書シリアル番号
cert.subjectaltname.upn	ユーザ 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。

クライアントレス SSL VPN 接続プロファイル、インターフェイスへの認可サーバ グループの割り当て

このダイアログボックスでは、インターフェイスを AAA サーバ グループに関連付けられます。結果は、[Authorization] ダイアログボックスのテーブルに表示されます。

- [Interface]：インターフェイスを選択します。デフォルトは DMZ です。
- [Server Group]：選択したインターフェイスに割り当てるサーバ グループを選択します。デフォルトは LOCAL です。
- [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。

接続プロファイル、アカウンティング

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

- [Accounting Server Group]：アカウンティングに使用するすでに定義済みのサーバ グループを選択します。
- [Manage]：AAA サーバ 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。

このダイアログのフィールドは AnyConnect クライアントおよびクライアントレス SSL VPN で同じですが、クライアントレス SSL VPN には追加のフィールドが 1 つあります。接続プロファイルのタブの名前は、AnyConnect では [Group URL/Group Alias] で、クライアントレス SSL VPN では [Clientless SSL VPN] 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 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。
- [Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored.)]：グループ URL に接続しているクライアントで Cisco Secure Desktop のアプリケーションを実行するかどうかを選択します。これらのオプションは、グループ URL を追加する場合にのみ表示されます。クライアントを免除すると、セキュリティ アプライアンスがこれらのユーザからエンドポイント基準を受信しなくなるので、ユーザが VPN にアクセスにできるように DAP コンフィギュレーションの変更が必要になることがあります。次のオプションから選択します。
  - [Always run CSD]：グループ URL に接続しているすべてのクライアントで Hostscan を実行します。

- [Disable CSD for both AnyConnect and clientless SSL VPN]：グループ URL に接続しているすべてのクライアントの Hostscan 処理を免除します。
- [Disable CSD for AnyConnect only]：グループ URL に接続している AnyConnect クライアントの Hostscan 処理を免除します。ただし、クライアントレス接続では Hostscan を使用します。

接続プロファイル、クライアントレス SSL VPN

[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] ダイアログボックスには、現在定義されているクライアントレス SSL VPN 接続プロファイルおよびグローバルのクライアントレス オプションが一覧表示されます。

- [Access Interfaces]：アクセスでイネーブルにするインターフェイスを選択できます。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。
  - [Device Certificate]：RSA キーまたは ECDSA キーまたはトラストポイントの認証の証明書を指定できます。2 つのトラストポイントを設定するオプションがあります。クライアントは、ベンダー ID ペイロードによる ECDSA のサポートを示します。ASA は、設定したトラストポイントリストをスキャンし、クライアントがサポートする最初の 1 つを選択します。ECDSA を使用する場合は、RSA トラストポイントの前に、このトラストポイントを設定する必要があります。
  - [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、または表示できます。
  - [Port Setting]：クライアントレス SSL および IPsec（IKEv2）接続のポート番号を設定します。範囲は 1 ～ 65535 です。デフォルトはポート 443 です。
- Login Page Setting
  - 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。選択しない場合は、DefaultWebVPNGroup が接続プロファイルになります。ユーザのログイン ページに、ユーザが接続で使用する特定のトンネル グループを選択するためのドロップダウン リストが表示されるように指定します。
  - [Allow user to enter internal password on the login page]：内部サーバへのアクセス時に異なるパスワードを入力するオプションを追加します。
  - [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]：この接続（トンネル グループ）の接続ポリシーを決定するレコードを示した接続テーブルを表示します。各レコードによって、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。

- [Add]：選択した接続の [Add Clientless SSL VPN] ダイアログボックスが開きます。
- [Edit]：選択した接続の [Edit Clientless SSL VPN] 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。
- [Name]：接続プロファイルの名前。
- [Enabled]：イネーブルになっている場合にチェックマークが付きます。
- [Aliases]：接続プロファイルの別名。
- [Authentication Method]：使用する認証方式を指定します。
- [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。

- [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、エンドポイントによって指定された推奨される値を、接続プロファイルによって指定された推奨される値と照合できない場合は、別の値と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。

クライアントレス SSL VPN 接続プロファイル、基本属性

[Clientless SSL VPN Connection Profile] > [Advanced] > [Basic] ダイアログボックスでは、基本属性を設定します。

- [Name]：接続名を指定します。編集機能の場合、このフィールドは読み取り専用です。
- [Aliases]：（任意）この接続の代替名を 1 つ以上指定します。[Clientless SSL VPN Access Connections] ダイアログボックスでそのオプションを設定している場合に、ログイン ページに別名が表示されます。
- [Authentication]：認証パラメータを指定します。
  - [Method]：この接続で、AAA 認証、証明書認証、またはその両方を使用するかどうかを指定します。デフォルトは AAA 認証です。
  - [AAA server Group]：この接続の認証処理で使用する AAA サーバグループを選択します。デフォルトは LOCAL です。

- [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。

- [DNS Server Group]：この接続の DNS サーバ グループとして使用するサーバを選択します。デフォルトは DefaultDNS です。
- [Default Group Policy]：この接続で使用するデフォルト グループ ポリシーのパラメータを指定します。
  - [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。
  - [Clientless SSL VPN Protocol]：この接続でのクライアントレス SSL VPN プロトコルをイネーブルまたはディセーブルにします。

クライアントレス SSL VPN 接続プロファイル、一般属性

[Clientless SSL VPN Connection Profile] > [Advanced] > [General] ダイアログボックスを使用して、AAA サーバに渡す前にユーザ名からレルムとグループを除去するかどうかを指定し、パスワード管理オプションを指定します。

- [Password Management]：AAA サーバからの 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 password management]：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に通知するかを決定します。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザ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、LDAP サーバなどの AAA サーバで有効です。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。

クライアントレス SSL VPN 接続プロファイル、認証

[Clientless SSL VPN Connection Profile] > [Advanced] > [Authentication] ダイアログボックスでは、インターフェイス固有の認可サーバ グループを表示、追加、編集、または削除できます。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 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 グループ、および選択したサーバ 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。

[Authentication] ペインのフィールドは、AnyConnect の認証と同じです（AnyConnect 接続プロファイル、認証属性 （69 ページ） を参照）。

クライアントレス SSL VPN 接続プロファイル、認証、サーバ グループの追加

[Clientless SSL VPN Connection Profile] > [Advanced] > [Authentication] ダイアログボックスの [Add] ボタンをクリックすると、インターフェイスを AAA サーバ グループに関連付けることができます。

この設定を行うフィールドについては、クライアントレス SSL VPN 接続プロファイル、インターフェイスへの認可サーバ グループの割り当て （79 ページ） を参照してください。

クライアントレス SSL VPN 接続プロファイル、2 次認証

クライアントレス SSL の 2 次認証設定フィールドは、接続プロファイル、2 次認証属性 （72 ページ） に記載されている AnyConnect クライアント アクセスと同様です。

クライアントレス SSL VPN 接続プロファイル、認可

クライアントレス SSL の認可設定フィールドは、AnyConnect、IKEv1、および IKEv2 の場合と同じです。これらのフィールドの詳細については、AnyConnect 接続プロファイル、認可属性（75 ページ）を参照してください。

クライアントレス SSL VPN 接続プロファイル、NetBIOS サーバ

クライアントレス SSL VPN 接続プロファイルの [Advanced] > [NetBIOS Servers] ダイアログボックスには、設定済みの NetBIOS サーバの属性が表示されます。[Add or Edit Tunnel Group dialog box for Clientless SSL VPN access] > [NetBIOS] ダイアログボックスを使用すれば、トンネル グループの NetBIOS 属性を設定することができます。クライアントレス SSL VPN では、NetBIOS と Common Internet File System（共通インターネット ファイル システム）プロトコルを使用して、リモート システム上のファイルにアクセスしたり、ファイルを共有したりします。Windows コンピュータにそのコンピュータ名を使用してファイル共有接続をしようとすると、指定されたファイル サーバはネットワーク上のリソースを識別する特定の NetBIOS 名と対応します。

ASA は、NetBIOS 名を IP アドレスにマップするために NetBIOS ネーム サーバにクエリーを送信します。クライアントレス SSL VPN では、リモート システムのファイルをアクセスまたは共有するための NetBIOS が必要です。

NBNS 機能を動作させるには、少なくとも 1 台の NetBIOS サーバ（ホスト）を設定する必要があります。冗長性を実現するために NBNS サーバを 3 つまで設定できます。ASA は、リストの最初のサーバを NetBIOS/CIFS 名前解決に使用します。クエリーが失敗すると、次のサーバが使用されます。

[NetBIOS Servers] ペインのフィールド

- [IP Address]：設定された NetBIOS サーバの IP アドレスを表示します。
- [Master Browser]：サーバが WINS サーバであるか、あるいは CIFS サーバ（つまりマスタブラウザ）にもなれるサーバであるかを表します。
- [Timeout (seconds)]：サーバが NBNS クエリーに対する応答を待つ最初の時間を秒単位で表示します。この時間を過ぎると、次のサーバにクエリーを送信します。
- [Retries]：設定されたサーバに対する NBNS クエリーの送信を順番にリトライする回数を表示します。言い換えれば、エラーを返すまでサーバのリストを巡回する回数ということです。最小リトライ数は 0 です。デフォルトの再試行回数は 2 回です。最大リトライ数は 10 です。
- [Add/Edit]：NetBIOS サーバを追加します。[Add or Edit NetBIOS Server] ダイアログボックスが開きます。
- [Delete]：選択した NetBIOS 行をリストから削除します。
- [Move Up/Move Down]：ASA は、このボックスに表示された順序で、NetBIOS サーバに NBNS クエリーを送信します。このボックスを使用して、クエリーをリスト内で上下に動かすことにより、優先順位を変更します。

クライアントレス SSL VPN 接続プロファイル、クライアントレス SSL VPN

クライアントレス接続プロファイルの [Advanced] > [Clientless SSL VPN] ペインでは、ログイン時にリモート ユーザに表示される内容に影響する属性を設定できます。

このダイアログと AnyConnect 接続プロファイルのフィールドは似ているため、詳細については接続プロファイル、グループ エイリアスとグループ URL （80 ページ）を参照してください。

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 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 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]：ユーザ認証で使用するサーバ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]：ユーザ認証で使用するサーバ 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 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 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 グループで障害が発生した場合に、ユーザ認証で 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 サーバの IP アドレスを指定します。最大で 10 台までのサーバ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 サーバに渡す前にユーザ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]：ユーザ名を AAA サーバに渡す前に、レルム（管理ドメイン）をユーザ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]：ユーザ名を AAA サーバに渡す前に、レルム（管理ドメイン）をユーザ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。ユーザ名<デリミタ>グループの形式でグループをユーザ名に追加します（例：JaneDoe@VPNGroup、JaneDoe#VPNGroup や JaneDoe!VPNGroup）。

- [Password Management]：AAA サーバからの 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 日前にユーザへの通知を開始し、以後、ユーザ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、LDAP サーバなどの AAA サーバで有効です。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 （67 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 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 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 サーバでグループ名が付加されたユーザのデータベースを維持しながら、同時にユーザ名のみに基づいてユーザ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 接続プロファイル、認証属性 （69 ページ）を参照してください。

IKEv1 接続プロファイル、アカウンティング

アカウン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、アカウンティング （79 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/Edi] > [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]：許容される 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ベースの 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、AnyConnect VPN クライアントに対する 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 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 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 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]：ユーザ認証で使用するサーバ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]：ユーザ認証で使用するサーバ 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 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 グループで障害が発生した場合に、ユーザ認証で 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 サーバの IP アドレスを指定します。最大で 10 台までのサーバ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 SSL VPN 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ると、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。

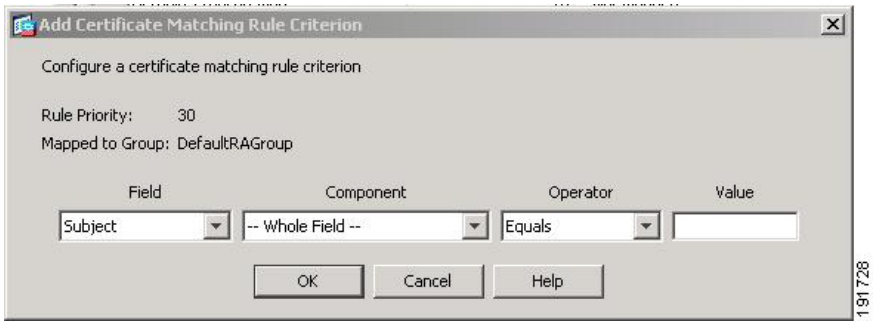
このペインには、証明書/接続プロファイルマップのリストとマッピング基準が表示されます。

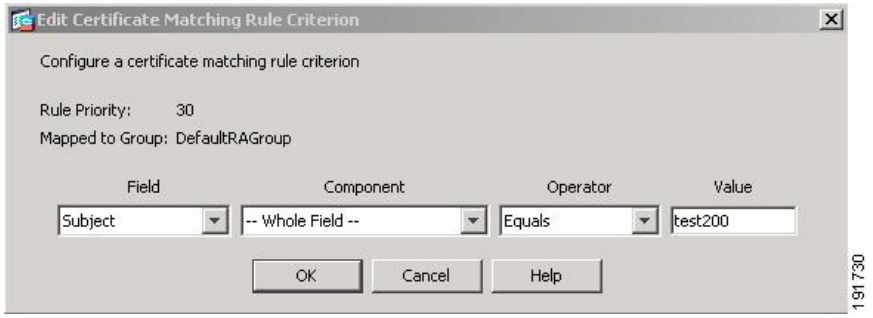
証明書/接続プロファイル マップ、証明書照合ルール基準の追加

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す。
Common Name（CN）	ユーザ、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、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に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 アドレッシングの LAN-to-LAN 接続については、両方のピアが Cisco ASA 5500 シリーズ セキュリティ アプライアンスの場合、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 Cisco ASA 5500 シリーズ 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。
  - [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。
  - この接続プロファイルには、[Advanced] > [Crypto Map Entry, and Adv] もあります。

Site-to-Site トンネル グループ

ASDM ペインの [Configuration] > [Site-to-Site VPN] > [Advanced] > [Tunnel Groups] では、IPsec Site-to-Site 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。

- [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。

AnyConnect VPN クライアント イメージ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect 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 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。

- [Add]：[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。
- [Replace]：[Replace 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 イメージとして指定して、[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。

AnyConnect VPN クライアント イメージ、追加/交換

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。

AnyConnect VPN クライアント イメージ、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 VPN クライアント接続の設定

AnyConnect クライアント プロファイルの設定

AnyConnect クライアント プロファイルをすべての AnyConnect ユーザにグローバルに展開するか、またはユーザのグループ ポリシーに基づいてユーザに展開するように ASA を設定できます。通常、ユーザは、インストールされている AnyConnect 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、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] で設定します。

[Add/Import]：[Add AnyConnect Client 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。

- [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にダウンロードされます。

[Edit]：[Edit SSL VPN Client Profile] 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 Client 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 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

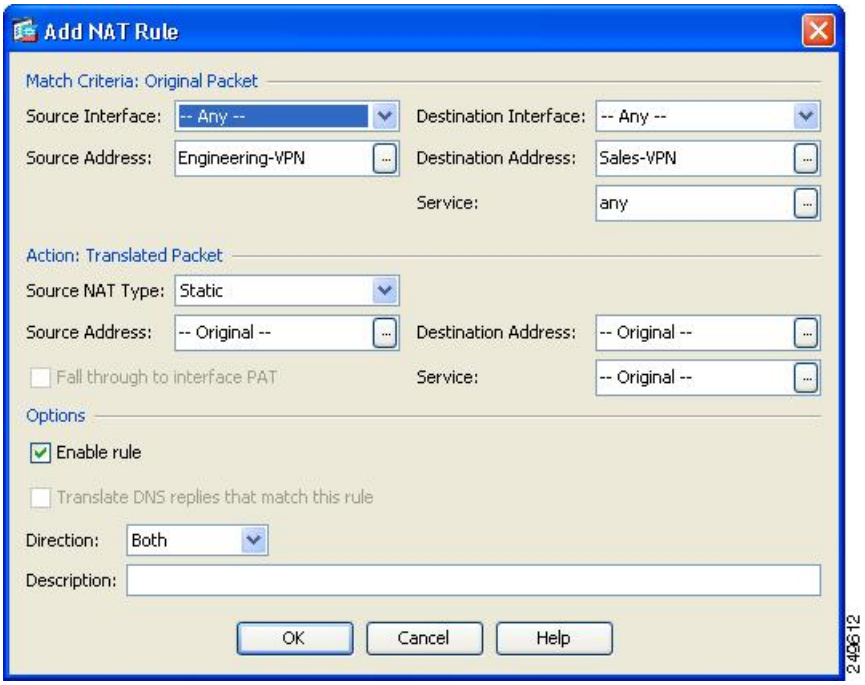
手順

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。

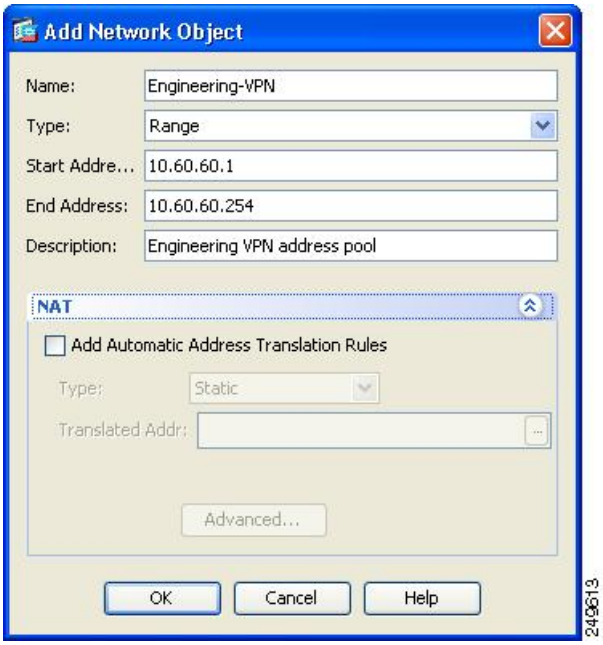
図 *1 : [Add NAT Rule]* ダイアログ ボックス



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) [適用（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
```

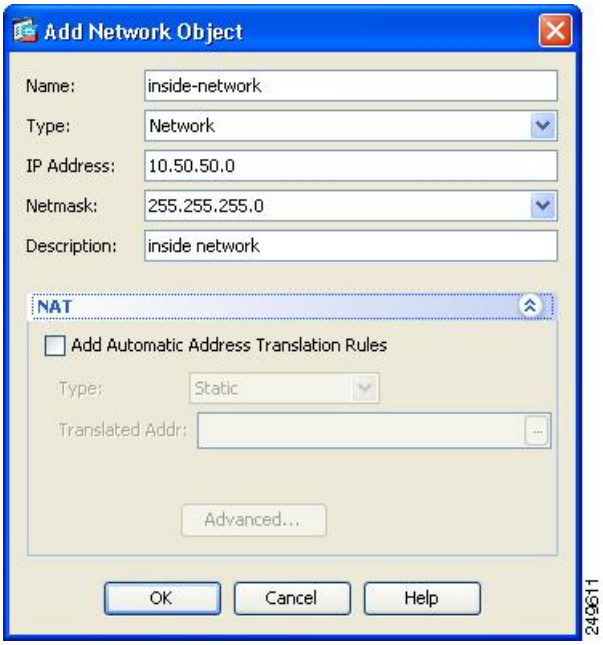
ステップ 4 Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。上記で規則を作成したときと同様にこの規則を作成します。ただし、[Match criteria: Original Packet] エリアで、Engineering VPN アドレス プールを送信元と宛先の両方のアドレスとして指定します。

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) [適用（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。

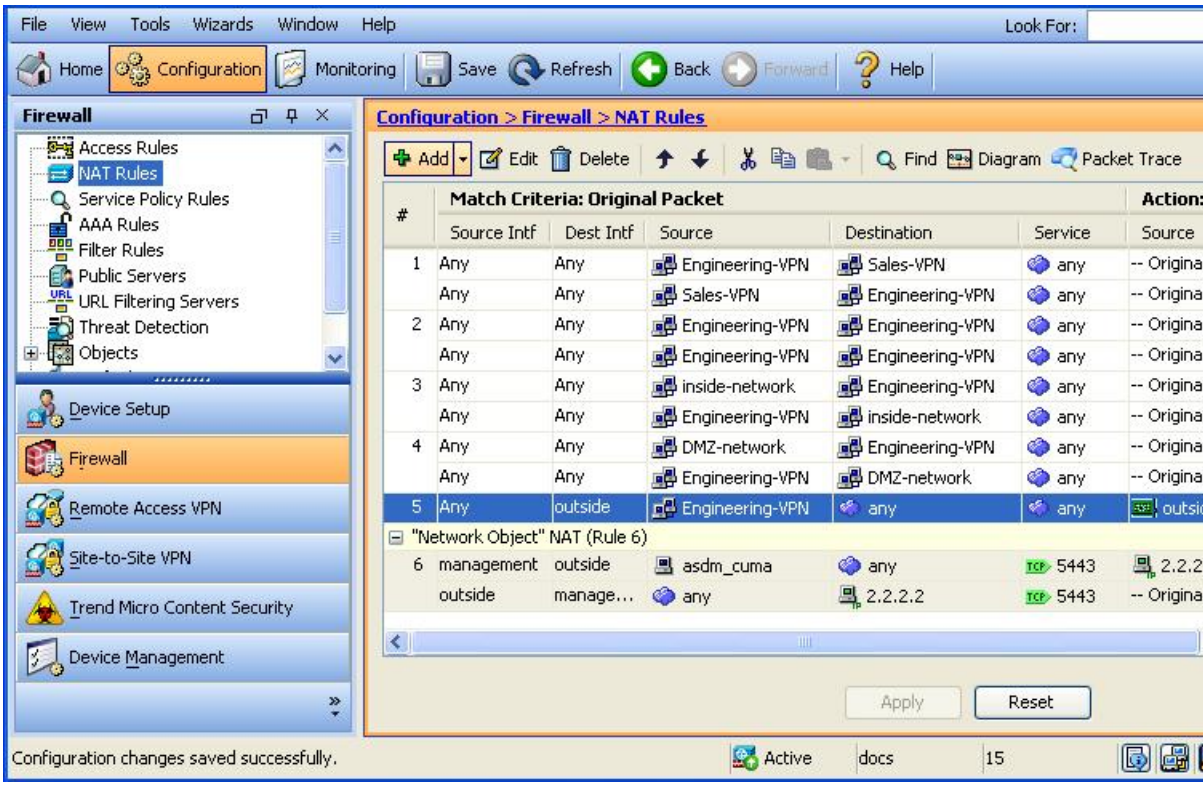
e) [OK] をクリックします。

f) [適用（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 HostScan

AnyConnect ポスチャ モジュールにより、AnyConnect Secure Mobility 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、および、アンチマルウェア、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、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 HostScan がインストールされている必要があります。

HostScan の前提条件

AnyConnect Secure Mobility Client をポスチャ 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

次の AnyConnect 機能は、ポスチャ モジュールをインストールする必要があります。

- SCEP 認証
- AnyConnect テレメトリ モジュール

ポスチャモジュール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 HostScan のライセンス

ポスチャ モジュールには、次の AnyConnect ライセンシング要件があります。

- 基本 HostScan 用 AnyConnect 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 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 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。

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ンタイム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 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 hostscan_version-k9.pkg ファイルをコンピュータにダウンロードします。

ステップ 2 ASDM を起動し、[Configuration][Remote Access VPN] > [Secure Desktop Manager] [Host Scan Image] > を選択します。

ステップ 3 [Upload] をクリックして、HostScan 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 [Upload Image] ダイアログボックスで [Browse Local Files] をクリックして、ローカル コンピュータ上の HostScan 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 ファイルを選択し、[Select] をクリックします。[Local File Path] フィールドと [Flash File System Path] フィールドで選択したファイルのパスは、HostScan 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 [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 パッケージ ファイルを使用します。

ステップ 9 [Enable HostScan] 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 のアンインストール

HostScan 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 が有効になっている場合でも ASA による HostScan パッケージの展開が回避されます。HostScan をアンインストールしても、HostScan 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、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan Image] > に移動して、HostScan をアンインストールします。

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 フィーチャ モジュールの割り当て

次の手順で、AnyConnect フィーチャ モジュールとグループ ポリシーを関連付けます。VPN ユーザが ASA に接続するときに、ASA はこれらの AnyConnect フィーチャ 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に AnyConnect フィーチャ 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 Module Name*

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）
websecurity	AnyConnect Web セキュリティ モジュール
telemetry	AnyConnect テレメトリ モジュール
posture	AnyConnect ポスチャ モジュール
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 の関連マニュアル

HostScan 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 の動作の詳細については、『Cisco *AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。

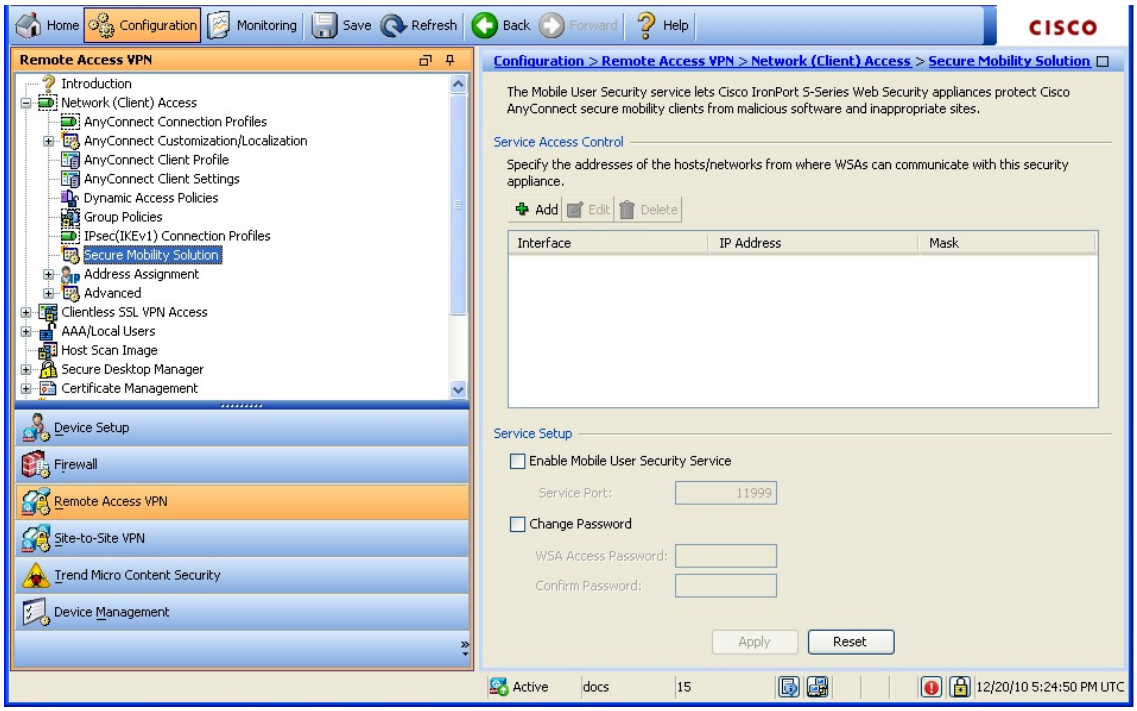
AnyConnect セキュア モビリティ ソリューション

AnyConnect セキュア モビリティは、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。AnyConnect Secure Mobility 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 Cisco AnyConnect セキュア モビリティ 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、Cisco AnyConnect セキュア モビリティ クライアントの AnyConnect セキュア モビリティ 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、AnyConnect Secure Mobility 機能をサポートする AnyConnect 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

[Configuration] > [Remote Access VPN] > [Network （Client） Access] > [Secure Mobility Solution] の下の [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 のカスタマイズとローカリゼーション

AnyConnect VPN クライアントをカスタマイズして、リモート ユーザに、会社のイメージを表示できます。[AnyConnect 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 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。

- [Import] をクリックすると、[Import AnyConnect 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。
- [Export] をクリックすると、[Export AnyConnect 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 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 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 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 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 Customization/Localization]：**[Binary]**

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 GUI および AnyConnect 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 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 Customization/Localization]：**[Script]**

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 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 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 AnyConnect Secure Mobility Client Administration Guide*』を参照してください。

AnyConnect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 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。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 AnyConnect Secure Mobility 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 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、クライアントのアップデートが利用可能になると、AnyConnect は更新を実行するか延期するかをユーザに尋ねるダイアログを開きます。詳細については、「Enable AnyConnect Client Deferred Upgrade」または『Cisco AnyConnect Secure Mobility Client Administration Guide』の「*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。

    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 ー 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 AnyConnect Secure Mobility 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には、属性名と値の両方を *true* に設定します。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 は次に管理トンネル接続に進みます。

- **no-dhcp-server-route**：（パブリック DHCP サーバルートを設定）このカスタム属性を使用すると、[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フローできます。AnyConnect は、AnyConnect クライアントが接続するとローカル DHCP サーバに特定のルートを追加してホスト マシンの LAN アダプタに暗黙的フィルタを適用し、そのルートについて DHCP トラフィック以外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 AnyConnect Secure Mobility Client Administration Guide』の「*Set Public DHCP Server Route*」の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 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 （30 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 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 AnyConnect Secure Mobility 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 Polices]** > 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 サーバのみがサポートされていますが、ユーザ インターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、ASA 上で別の Integrity サーバを設定して、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 IP アドレスを Integrity サーバ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]：選択したサーバを Integrity サーバのリストから削除します。
- [Move Up]：選択したサーバを Integrity サーバ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]：選択したサーバを Integrity サーバ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 サーバの設定を適用します。
- [Reset]：まだ適用されていない Integrity サーバ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、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザ 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
- L2TP/IPSec

システム フローは次のとおりです。

1. エンド ユーザが VPN 接続を要求します。
2. ASA は、ISE に対してユーザを認証し、ネットワークへの限定アクセスを提供するユーザ ACL を受け取ります。

3. アカウンティング開始メッセージが 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 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 サーバを含むサーバ 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 グループを使用します。

手順

ステップ 1 ISE サーバの RADIUS AAA サーバ 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 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 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 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 グループを使用すると、対応する RADIUS サーバ 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 グループを認可に使用するときに、RADIUS アクセス要求メッセージが、AAA サーバ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 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ティングにこのサーバ 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 グループを保存します。

i) サーバ 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、サーバをグループに追加します。

サーバ グループに別の ISE サーバを追加します。

ステップ 2 リモート アクセス VPN で ISE サーバ 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) **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect 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 グループを選択します。

- 許可用にのみ ISE サーバ 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 グループを選択します。
e) **[Advanced]** > **[Accounting]** ページで、ISE サーバ 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。