CHAPTER 3

VPN アクセスの設定

ここでは、Cisco AnyConnect Secure Mobility Client の VPN プロファイルと機能、およびそれらの設定方法について説明します。

- 「AnyConnect VPN プロファイル エディタのパラメータに関する説明」（P.3-80）

AnyConnect クライアントの IP アドレスの設定

インターネットワーク接続は、IP アドレスによって可能になります。IP アドレスは、送信者と受信者の両方に接続用の番号が割り当てられている必要があるという点で、電話番号に似ています。ただし、VPN では、実際には 2 セットのアドレスが存在します。最初のセットは、パブリック ネットワーク上でクライアントとサーバを接続します。この接続が確立されると、2 番目のセットが VPN トンネル経由でクライアントとサーバを接続します。

ASA のアドレス管理では、この IP アドレスの 2 番目のセットを扱います。これらのプライベート IP アドレスは、クライアントをトンネル経由でプライベート ネットワーク上のリソースに接続し、プライベート ネットワークに直接接続されているかのようなクライアント機能を提供します。また、ここでは、クライアントに割り当てられたプライベート IP アドレスのみを扱います。プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、VPN 管理ではなく、ネットワーク管理業務の一部に位置づけられます。したがって、ここで IP アドレスに言及する場合は、クライアントをトンネルのエンドポイントとして機能させる、プライベート ネットワークのアドレッシング方式で取得される IP アドレスを意味します。

この項は、次の内容で構成されています。

- 「IP アドレスの割り当てポリシー」（P.3-2）
- 「内部 IP アドレス プール」（P.3-3）
- 「IP アドレスの AnyConnect 接続への割り当て」（P.3-5）

IP アドレスの割り当てポリシー

- [Use authentication server]：ユーザ単位で外部認証、認可、アカウンティング サーバからアドレスを取得します。IP アドレスが設定された認証サーバを使用している場合は、この方式を使用することをお勧めします。[Configuration] > [AAA Setup] ペインで AAA サーバを設定できます。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
- [Use DHCP]：DHCP サーバから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバを設定する必要があります。また、DHCP サーバで使用可能な IP アドレスの範囲も定義する必要があります。DHCP を使用する場合は、[Configuration] > [Remote Access VPN] > [DHCP Server] ペインでサーバを設定します。この方法は IPv4 の割り当てポリシーに使用できます。
- [Use an internal address pool]：内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方法を使用する場合は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] ペインで IP アドレス プールを設定します。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
  - [Allow the reuse of an IP address so many minutes after it is released]：IP アドレスがアドレス プールに戻された後に、IP アドレスを再利用するまでの時間を指定します。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、これはチェックされません。つまり、ASA は遅延時間を課しません。遅延時間を設定する場合は、チェックボックスをオンにし、IP アドレスを再割り当てするまでの時間を 1 ～ 480 の範囲で指定します。この設定要素は IPv4 の割り当てポリシーに使用できます。

ASDM を使用した IPv4 および IPv6 のアドレス割り当ての設定

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] を選択します。

ステップ 2　[IPv4 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server] : IP アドレスを提供するために設定した認証、許可、アカウンティング（AAA）サーバを使用できるようにします。
- [Use DHCP] : IP アドレスを提供するために設定したダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバを使用できるようにします。
- [Use internal address pools] : ASA で設定されたローカル アドレス プール設定を使用できるようにします。

[Use internal address pools] を有効にする場合、IPv4 アドレスが解放された後、そのアドレスの再利用を有効にできます。IP v4 アドレスが再利用できるようになる時間範囲を 0 ～ 480 分から指定できます。

ステップ 3　[IPv6 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server] : IP アドレスを提供するために設定した認証、許可、アカウンティング（AAA）サーバを使用できるようにします。
- [Use internal address pools] : ASA で設定されたローカル アドレス プール設定を使用できるようにします。

ステップ 4　[Apply] をクリックします。

ステップ 5　[OK] をクリックします。

内部 IP アドレス プール

VPN リモート アクセス トンネルを使用するよう IPv4 または IPv6 アドレス プールを設定するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] > [Add/Edit IP Pool] を選択します。

アドレス プールを削除するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] を選択します。削除するアドレス プールを選択し、[Delete] をクリックします。

ASA は、接続の接続プロファイルまたはグループ ポリシーに基づいてアドレス プールを使用します。プールの指定順序は重要です。接続プロファイルまたはグループ ポリシーに複数のアドレス プールを設定する場合、ASA はそれらを ASA に追加した順序で使用します。

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

（注）　IPv4 および IPv6 両方の ASA の外部インターフェイス アドレスは、アドレス プールで定義されているようにプライベート側のアドレス空間と重複できません。

ASDM を使用したローカル IPv4 アドレス プールの設定

[IP Pool] エリアには、設定された各アドレス プールが、名前ごとに、それぞれの IP アドレス範囲（たとえば、10.10.147.100 ～ 10.10.147.177）とともに表示されます。プールが存在しない場合、エリアは空です。ASA は、リストに表示される順番でこれらのプールを使用します。最初のプールのすべてのアドレスが割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

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

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。

ステップ 2　IPv4 アドレスを追加するには、[Add] > [IPv4 Address pool] をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、[Edit] をクリックします。

ステップ 3　[Add/Edit IP Pool] ダイアログボックスで、次の情報を入力します。

- [Pool Name]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [Starting Address]：設定されたそれぞれのプールで使用可能な最初の IP アドレスを示します。たとえば 10.10.147.100 のように、ドット付き 10 進数表記を使用します。
- [Ending Address]：設定されたそれぞれのプールで使用可能な最後の IP アドレスを示します。たとえば 10.10.147.177 のように、ドット付き 10 進数表記を使用します。
- [Subnet Mask]：この IP アドレスが常駐するサブネットを指定します。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックします。

ASDM を使用したローカル IPv6 アドレス プールの設定

[IP Pool] エリアには、設定された各アドレス プールが、名前ごとに、開始 IP アドレス範囲、アドレス プレフィックス、プールに設定できるアドレス数とともに表示されます。プールが存在しない場合、エリアは空です。ASA は、リストに表示される順番でこれらのプールを使用します。最初のプールのすべてのアドレスが割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

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

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。

ステップ 2　IPv6 アドレスを追加するには、[Add] > [IPv6 Address pool] をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、[Edit] をクリックします。

ステップ 3　[Add/Edit IP Pool] ダイアログボックスで、次の情報を入力します。

- [Name]：設定された各アドレス プールの名前を表示します。
- [Starting IP Address]：設定されたプールで使用可能な最初の IP アドレスを入力します。たとえば、2001:DB8::1 となります。
- [Prefix Length]：IP アドレス プレフィックス長をビット単位で入力します。たとえば、32 は CIDR 表記で /32 を表します。プレフィックス長は、IP アドレスが常駐するプールのサブネットを定義します。

- [Number of Addresses]：開始 IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックします。

IP アドレスの AnyConnect 接続への割り当て

次のいずれかの方法で IP アドレスを VPN 接続に割り当てます。

- 「内部アドレス プールを使用した IP アドレスの割り当て」（P.3-5）：内部プールはグループ ポリシーに関連付けられており、ASA で設定されています。IPv4 アドレスまたは IPv6 アドレスが使用できます。
- 「DHCP を使用した IP アドレスの割り当て」（P.3-6）：DHCP サーバを ASA で設定されているグループ ポリシーに関連付けます。IPv4 アドレスのみ使用できます。
- 「IP アドレスのローカル ユーザへの割り当て」（P.3-6）：IP アドレスを ASA で設定されたユーザに割り当てます。IPv4 アドレスまたは IPv6 アドレスが使用できます。

内部アドレス プールを使用した IP アドレスの割り当て

[Add or Edit Group Policy] ダイアログボックスでは、追加または編集している内部ネットワーク（クライアント）アクセス 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。

同じグループ ポリシーで IPv4 と IPv6 両方のアドレス ポリシーを設定できます。同じグループ ポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

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] を選択します。

ステップ 2　新しいグループ ポリシーまたは内部アドレス プールで設定するグループ ポリシーを作成し、[Edit] をクリックします。

[General attributes] ペインは [group policy] ダイアログで、デフォルトで選択されています。

ステップ 3　[Address Pools] フィールドを使用して、このグループ ポリシーの IPv4 アドレス プールを指定します。[Select] をクリックし、IPv4 アドレス プールを追加または編集します。詳細については、「ASDM を使用したローカル IPv4 アドレス プールの設定」（P.3-4）を参照してください。

ステップ 4　[IPv6 Address Pools] フィールドを使用して、このグループ ポリシーに使用する IPv6 アドレス プールを指定します。[Select] をクリックし、IPv6 アドレス プールを追加または編集します。「ASDM を使用したローカル IPv6 アドレス プールの設定」（P.3-4）を参照してください。

ステップ 5　[OK] をクリックします。

ステップ 6　[Apply] をクリックします。

DHCP を使用した IP アドレスの割り当て

DHCP サーバを使用して IPv4 アドレスを割り当てるには、以下の指示に従って DHCP を使用するよう IP アドレス割り当てポリシーを設定します。DHCP サーバを使用して IPv6 アドレスを AnyConnect クライアントに割り当てることはできません。

ステップ 1　ASDM を使用して ASA に接続します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] を選択します。

ステップ 3　[Use DHCP] をクリックします。

ステップ 4　[Apply] をクリックします。

ステップ 5　[Configuration] > [Remote Access VPN] > [DHCP Server] を選択して、DHCP サーバを設定します。

IP アドレスのローカル ユーザへの割り当て

ASA 管理者は、ASA の個々のユーザのアカウントを作成できます。これらのアカウントはグループ ポリシーを使用するよう設定したり、特にローカル ユーザ ポリシーで設定されたグループ ポリシーで検出された同じ VPN 属性を多数持ったりすることができます。またこれら個々のユーザのアカウントに、AnyConnect 属性をいくつか設定させることができます。

ここでは、ローカル ユーザのすべての属性を設定する方法について説明します。

前提条件

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、『*Cisco ASA 5500 Configuration Guide Using ASDM*』の第 42 章「Configuring AAA Servers and the Local Database」の「Adding a User Account to the Local Database」を参照してください。

ガイドライン

デフォルトでは、[Edit User Account] 画面の設定ごとに [Inherit] チェックボックスがオンになっています。つまり、ユーザ アカウントは、デフォルト グループ ポリシー DfltGrpPolicy のその設定の値を継承するということです。

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。次の「手順の詳細」で、[Edit User Account] 画面の各設定について説明しています。

手順の詳細

ステップ 1　ASDM を開始し、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択します。

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。

[Edit User Account] 画面が開きます。

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、使用できる VPN トンネリング プロトコルを選択します。選択されたプロトコルのみが使用可能になります。次の選択肢があります。

- （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 Secure Mobility Client 対応の IPsec IKEv2。IKEv2 を使用した IPsec による AnyConnect 接続では、SSL VPN 接続が使用できる同じ機能セットを利用できます。
- L2TP over IPSec では、複数の PC やモバイル PC に採用されている一般的なオペレーティング システムに付属の VPN クライアントを使用するリモート ユーザが、パブリック IP ネットワークを介して 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るようにします。

（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、ASA を経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。フィルタおよび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] を選択します。

[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。同一ではなかった場合、ASA はユーザによる接続を禁止します。[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、パスワードの保存は*許可しない*ことを推奨します。

ステップ 9　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。

ステップ 10　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）　最大値を設定して制限しておかない同時に多数の接続が許可されるため、セキュリティとパフォーマンスの低下を招くおそれがあります。

ステップ 11　ユーザ接続時間の**最大接続時間**を分で指定します。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。最短時間は 1 分、最長時間は 2147483647 分（4000 年超）です。接続時間を無制限にするには、[Unlimited] チェックボックスをオンにします（デフォルト）。

ステップ 12　ユーザのアイドル タイムアウトを分で指定します。この期間、このユーザの接続に通信アクティビティがなかった場合、システムは接続を終了します。最短時間は 1 分で、最長時間は 10080 分です。この値は、クライアントレス SSL VPN 接続のユーザには適用されません。

ステップ 13　セッション アラート間隔を設定します。[Inherit] チェックボックスをオフにすると、自動的に [Default] チェックボックスがオンになります。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] チェックボックスをオフにして、セッション アラート間隔（1 ～ 30 分）を分数ボックスで指定します。

ステップ 14　アイドル アラート間隔を設定します。[Inherit] チェックボックスをオフにすると、自動的に [Default] チェックボックスがオンになります。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] チェックボックスをオフにして、セッション アラート間隔（1 ～ 30 分）を分数ボックスで指定します。

ステップ 15　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] 領域（任意）で、IPv4 アドレスおよびサブネット マスクを入力します。

ステップ 16　このユーザに対して専用の IPv6 アドレスを設定する場合は、[Dedicated IPv6 Address] フィールド（任意）で、IPv6 アドレスを IPv6 プレフィックスとともに入力します。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 17　クライアントレス SSL の設定を行う場合は、左側のペインで、[Clientless SSL VPN] をクリックします。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。

ステップ 18　[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。

IPv4 または IPv6 トラフィックを設定して VPN をバイパスする

クライアント バイパス プロトコル機能により、ASA で IPv6 トラフィックのみ予想されている場合に AnyConnect クライアントが IPv4 トラフィックを管理する方法、または ASA で IPv4 トラフィックのみ予想されている場合に AnyConnect が IPv6 トラフィックを管理する方法を設定できます。

AnyConnect クライアントで ASA に VPN 接続をする場合、ASA はクライアントに IPv4、IPv6、または IPv4 および IPv6 両方のアドレスを割り当てる場合があります。

クライアント バイパス プロトコルが 1 つの IP プロトコルに対して有効で、そのプロトコルにアドレス プールが設定されていない（つまり、そのプロトコルの IP アドレスが ASA からクライアントにプッシュされていなかった）場合、そのプロトコルを使用した IP トラフィックは VPN トンネル経由で送信されず、クリア テキストで AnyConnect クライアントから送信されます。

一方、クライアント バイパス プロトコルが無効で、そのプロトコルにアドレス プールが設定されていない場合、VPN トンネルが確立されると、その IP プロトコルのすべてのトラフィックがドロップされます。

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。エンドポイントが IPv6 アドレスに達しようとするときにクライアント バイパス プロトコルが無効な場合、IPv6 トラフィックはドロップされ、クライアント バイパス プロトコルが有効な場合、IPv6 トラフィックはクリア テキストでクライアントから送信されます。

クライアント バイパス プロトコルを ASA でグループ ポリシーに対して設定します。

ステップ 1　ASDM を使用して ASA に接続します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 3　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 4　[Advanced] > [AnyConnect] を選択します。

ステップ 5　デフォルト グループ ポリシー以外のグループ ポリシーの場合、[Client Bypass Protocol] の隣にある [Inherit] のチェックボックスをオフにします。

ステップ 6　次のオプションのいずれかを選択します。

- ASA がアドレスを割り当てなかった IP トラフィックをドロップする場合は、[Disable] をクリックします。
- その IP トラフィックをクリア テキストで送信する場合は、[Enable] をクリックします。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。

AnyConnect プロファイルの設定と編集

ここでは、ASDM からプロファイル エディタを起動する方法、およびプロファイルを新規作成する方法について説明します。

Cisco AnyConnect Secure Mobility Client ソフトウェア パッケージ バージョン 2.5 以降（すべてのオペレーティング システム用）にはプロファイル エディタが含まれています。プロファイル エディタは、ASA 上で AnyConnect ソフトウェア パッケージを SSL VPN クライアント イメージとしてロードした時点で ASDM によりアクティブ化されます。

複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージからプロファイル エディタがロードされます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の AnyConnect で使用される機能が表示されます。

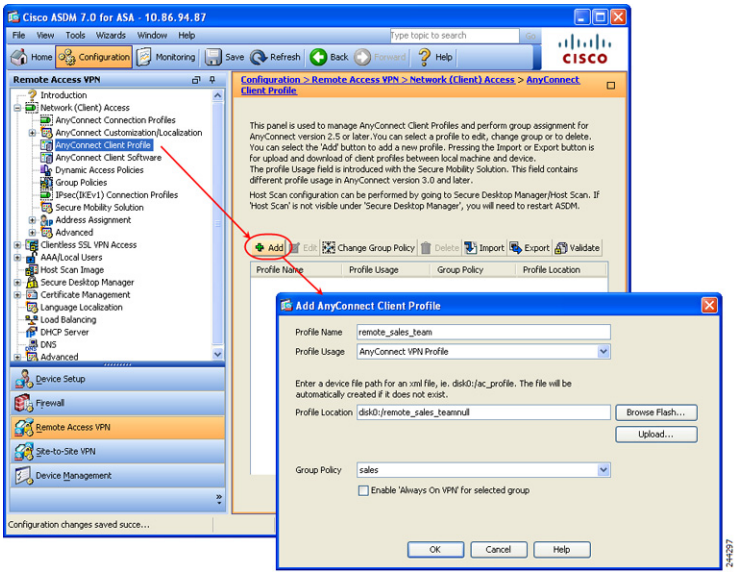
ASDM でプロファイル エディタをアクティブ化する手順は次のとおりです。

ステップ 1　AnyConnect ソフトウェア パッケージを AnyConnect Client イメージとしてロードします。まだロードしていない場合は、第 2 章「AnyConnect をダウンロードするための ASA の設定」を参照してください。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。[AnyConnect Client Profile] ペインが開きます。

ステップ 3　[Add] をクリックします。[Add AnyConnect Client Profile] ウィンドウが開きます（図 3-1）。

図 3-1　AnyConnect プロファイルの追加



ステップ 4　プロファイル名を指定します [Profile Location] で別の値を指定しない限り、ASDM では XML ファイルが ASA のフラッシュ メモリ上に同じ名前で作成されます。

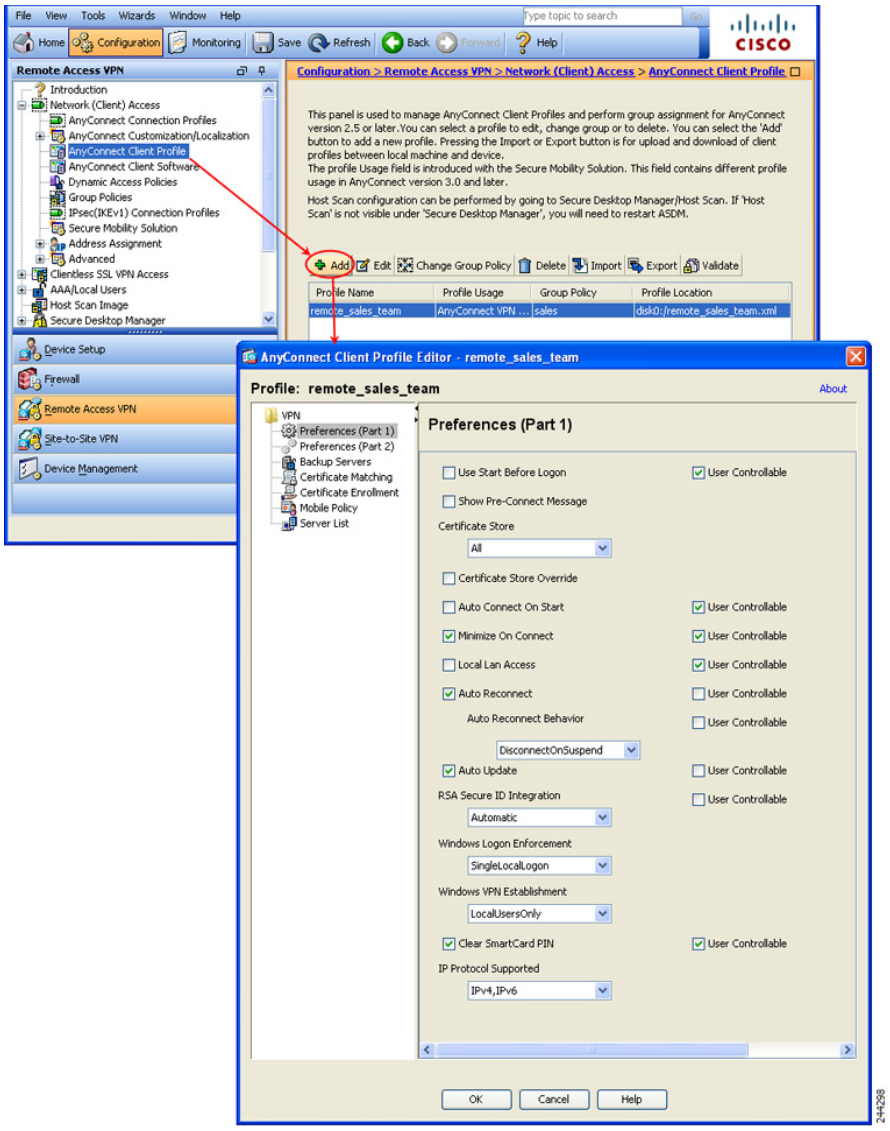
（注）　名前を指定するときに、.xml 拡張子は含めないでください。プロファイルに example.xml という名前を付けた場合、ASDM により自動的に .xml 拡張子が追加されて、名前が example.xml.xml に変更されます。この場合、ASA の [Profile Location] フィールドで名前を example.xml に変更しても、リモート アクセスで AnyConnect に接続したときに、名前は example.xml.xml に戻ってしまいます。（.xml 拡張子の重複により）AnyConnect がプロファイル名を認識できない場合、IKEv2 接続は失敗する場合があります。

ステップ 5　グループ ポリシーを選択します（任意）。ASA は、このプロファイルをグループ ポリシー内の全 AnyConnect ユーザに適用します。

ステップ 6　[OK] をクリックします。ASDM によりプロファイルが作成され、そのプロファイルはプロファイル テーブルに表示されます。

ステップ 7　作成されたばかりのプロファイルをプロファイル テーブルから選択します。[Edit] をクリックします。プロファイル エディタは図 3-2 のように表示されます。プロファイル エディタの各ペインで、AnyConnect 機能を有効にします。終了したら、[OK] をクリックします。

図 3-2　プロファイルの編集



AnyConnect プロファイルの展開

（注）　クライアント GUI に、最初の VPN 接続でユーザが制御可能な設定がすべて表示されるように、プロファイルのホスト リストには ASA を含める必要があります。ASA のアドレスまたは FQDN をホスト エントリとしてプロファイルに追加していない場合、フィルタがセッションに適用されません。たとえば、証明書照合を作成し、証明書が基準と適切に一致した場合でも、プロファイルに ASA をホスト エントリとして追加しなかった場合、この証明書照合は無視されます。プロファイルへのホスト エントリの追加の詳細については、「サーバ リストの設定」（P.3-60）を参照してください。

ステップ 1　クライアント プロファイルとグループ ポリシーを関連付けます。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 2　新しいグループ ポリシーを追加するか、グループ ポリシー テーブルからグループ ポリシーを選択し、[Edit] をクリックします。

ステップ 3　[Advanced] > [AnyConnect Client] の順に選択します。

ステップ 4　[Inherit] チェックボックスをオフにし、[Select AnyConnect Client Profile] ダイアログボックスを使用して、ダウンロードする AnyConnect プロファイルを選択します。

ステップ 5　設定が完了したら、[OK] をクリックし、[Apply] をクリックします。

VPN ロード バランシングの設定

AnyConnect クライアントのロード バランシングの設定は、『*Cisco ASA 5500 Series Configuration Guide using ASDM, 6.4 and 6.6*』の第 67 章「Configuring IKE, Load Balancing, and NAC」の「Configuring Load Balancing」ですべて説明しています。

そこで定義されているガイドラインに加えて、次のガイドラインに注目してください。

- IPv6 アドレスを使用したクライアントは、ASA クラスタの公開されている IPv6 アドレス経由または GSS サーバ経由で AnyConnect 接続を行うことができます。同様に、IPv6 アドレスを使用したクライアントは、ASA クラスタの公開されている IPv4 アドレス経由または GSS サーバ経由で AnyConnect VPN 接続を行うことができます。どちらのタイプの接続も ASA クラスタ内でロード バランシングできます。

  IPv6 アドレスを使用したクライアントが ASA の公開されている IPv4 アドレスに正常に接続するには、IPv6 から IPv4 へネットワーク アドレス変換が可能なデバイスがネットワークに存在する必要があります。

- AnyConnect でロード バランシングの証明書確認を実行し、IP アドレスによって接続がリダイレクトされている場合、クライアントにより、この IP アドレスを通してその名前チェックがすべて実行されます。お客様は、この IP アドレスが証明書の一般名、つまり **subject alt name** に一覧表示されていることを確認する必要があります。IP アドレスがこれらのフィールドに存在しない場合、証明書は非信頼と見なされます。

- RFC 2818 で定義されたガイドラインに従って、**subject alt name** が証明書に組み込まれている場合、名前チェックにのみ **subject alt name** を使用し、一般名は無視します。証明書を提示しているサーバの IP アドレスが証明書の **subject alt name** で定義されていることを確認します。

スタンドアロン ASA の場合、IP アドレスはその ASA の IP です。クラスタリング環境では、証明書の設定により異なります。クラスタで使用されている証明書が 1 つの場合、それがクラスタの IP になり、証明書には Subject Alternative Name 拡張子があり、それぞれ ASA の IP と FQDN を持っています。クラスタで使用されている証明書が複数の場合、それが再度 ASA の IP アドレスになるはずです。

Start Before Logon の設定

Start Before Logon（SBL）によりユーザは、Windows へのログイン前に、企業インフラへの VPN 接続を確立できます。

Windows ログインでは、Windows 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、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。ASA で認証が行われると、Windows ログイン ダイアログが表示され、ユーザは通常どおりにログインします。SBL は Windows でのみ使用可能で、ログイン スクリプト、パスワードのキャッシュ、ネットワーク ドライブからローカル ドライブへのマッピングなどの使用を制御できます。

（注） AnyConnect は、Windows XP x64（64 ビット）Edition 用の SBL をサポートしていません。

SBL を有効にする理由としては、次のものがあります。

- ユーザのコンピュータに Active Directory インフラストラクチャを導入済みである。
- コンピュータのキャッシュにクレデンシャルを入れることができない（グループ ポリシーでキャッシュのクレデンシャル使用が許可されない場合）。
- ネットワーク リソースから、またはネットワーク リソースへのアクセスを必要とする場所からログイン スクリプトを実行する必要がある。
- ネットワークでマッピングされるドライブを使用し、Microsoft Active Directory インフラストラクチャの認証を必要とする。
- インフラストラクチャとの接続を必要とする場合があるネットワーキング コンポーネント（MS NAP/CS NAC など）が存在する。

SBL 機能を有効にするには、AnyConnect プロファイルを変更して、ASA が SBL 用の AnyConnect モジュールをダウンロードできるようにする必要があります。

SBL に必要な設定は、この機能を有効にすることだけです。ログイン前に実施されるこのプロセスは、ネットワーク管理者がそれぞれの状況の要件に基づいて処理します。ログイン スクリプトは、ドメインまたは個々のユーザに割り当てることができます。通常ドメインの管理者は、バッチ ファイルまたはそれに類するものを Microsoft Active Directory のユーザまたはグループに定義しています。ユーザがログインするとすぐに、ログイン スクリプトが実行されます。

SBL を使用すると、ローカルの社内 LAN 上にあるものと同等のネットワークを構成できます。たとえば、SBL を有効にすると、ユーザはローカルのインフラストラクチャにアクセスできるため、通常はオフィス内のユーザが実行するログイン スクリプトをリモート ユーザからも使用できるようになります。これには、ドメイン ログイン スクリプト、グループ ポリシー オブジェクト、およびユーザがシステムにログインするときに通常実行されるその他の Active Directory 機能が含まれます。

これ以外の例として、コンピュータへのログインに使用するキャッシュ クレデンシャルを許可しないようにシステムを設定する場合があります。このシナリオでは、コンピュータへのアクセスが許可される前にユーザのクレデンシャルが確認されるようにするため、ユーザは社内ネットワーク上のドメイン コントローラと通信できることが必要です。

SBL は、呼び出されたときにネットワークに接続されている必要があります。場合によっては、ワイヤレス接続がワイヤレス インフラストラクチャに接続するユーザのクレデンシャルに依存するために、接続できないことがあります。このシナリオでは、ログインのクレデンシャル フェーズよりも SBL モードが優先されるため、接続できません。このような場合に SBL を機能させるには、ログインを通してクレデンシャルをキャッシュするようにワイヤレス接続を設定するか、またはその他のワイヤレス認証を設定する必要があります。ネットワーク アクセス マネージャがインストールされている場合、マシン接続を展開して、適切な接続を確実に使用できるようにする必要があります。詳細については、第 4 章「ネットワーク アクセス マネージャの設定」を参照してください。

AnyConnect は、高速ユーザ切り替えと互換性がありません。

この項では、次のトピックについて取り上げます。

Start Before Logon コンポーネントのインストール（Windows のみ）

Start Before Logon コンポーネントは、コア クライアントのインストール*後*にインストールする必要があります。また、Start Before Logon コンポーネントには、コア クライアント コンポーネントをインストールする必要があります。MSI ファイルを使用して AnyConnect および Start Before Logon コンポーネントを事前に展開する場合（Altiris、Active Directory、SMS など独自のソフトウェア展開手段を持つ大企業の場合など）は、正しい順序でインストールする必要があります。インストールの順序は、Web 展開または Web 更新されている AnyConnect を管理者がロードした時点で自動的に処理されます。

（注）　AnyConnect は、サードパーティの Start Before Logon アプリケーションでは起動できません。

Windows のバージョン違いによる Start Before Logon の差異

Windows 7 および Vista システムでは、SBL の有効化の手順が一部異なります。Vista よりも前のシステムでは、VPNGINA（virtual private network graphical identification and authentication の略称）というコンポーネントにより SBL が実装されていました。Windows 7 および Vista システムでは、SBL の実装に PLAP という名前のコンポーネントが使用されます。

AnyConnect では、Windows 7 または Vista の SBL 機能は Pre-Login Access Provider（PLAP）と呼ばれます。これは、接続可能なクレデンシャル プロバイダーです。この機能を使用すると、ネットワーク管理者は、クレデンシャルの収集やネットワーク リソースへの接続など特定のタスクをログイン前に実行することができます。Windows 7 および Windows Vista の SBL 機能は、PLAP により実現されます。PLAP は、vpnplap.dll を使用する 32 ビット版のオペレーティング システムと、vpnplap64.dll を使用する 64 ビット版のオペレーティング システムをサポートしています。PLAP 機能は、Windows 7 および Vista の x86 バージョンおよび x64 バージョンをサポートします。

（注）　この項で説明する VPNGINA とは Vista 以前のプラットフォームの Start Before Logon 機能を指し、PLAP は Windows 7 および Vista システムの Start Before Logon 機能を指します。

GINA は、ユーザが Ctrl キー、Alt キー、および Del キーを同時に押すと起動します。PLAP では、Ctrl キー、Alt キー、および Del キーを同時に押すとウィンドウが表示され、そこでシステムにログインするか、ウィンドウの右下隅にある [Network Connect] ボタンで任意のネットワーク接続（PLAP コンポーネント）を起動するかを選択できます。

以下の項では、VPNGINA と PLAP SBL の設定および手順について説明します。Windows 7 プラットフォームまたは Windows Vista プラットフォームにおける SBL 機能（PLAP）の有効化および使用に関する詳細については、「Windows 7 システムおよび Windows Vista システムでの Start Before Logon（PLAP）の設定」（P.3-16）を参照してください。

AnyConnect プロファイルでの SBL の有効化

AnyConnect プロファイルで SBL を有効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Preferences] ペインに移動し、[Use Start Before Logon] をオンにします。

ステップ 3　（任意）リモート ユーザが SBL の使用を制御できるようにする場合は、[User Controllable] をオンにします。

（注）　SBL を有効にする場合は、その前にユーザがリモート コンピュータをリブートする必要があります。

セキュリティ アプライアンスでの SBL の有効化

ダウンロード時間を最小限に抑えるため、AnyConnect は、サポートされる各機能に必要なコア モジュールだけ（ASA から）ダウンロードするよう要求します。SBL を有効にするには、ASA のグループ ポリシーで、SBL モジュール名を指定する必要があります。手順は次のとおりです。

ステップ 1　[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　左側のナビゲーション ペインで [Advanced] > [AnyConnect Client] を選択します。AnyConnect Client 設定が表示されます。

ステップ 4　[Optional Client Module for Download] 設定の [Inherit] をオフにします。

ステップ 5　ドロップダウン リストから **AnyConnect SBL** モジュールを選択します。

SBL に関するトラブルシューティング

SBL で問題が発生した場合は、次の手順に従ってください。

ステップ 1　AnyConnect プロファイルが ASA にロードされており、展開できるようになっていることを確認します。

ステップ 2　以前のプロファイルを削除します（*.xml と指定してハード ドライブ上の格納場所を検索します）。

ステップ 3　Windows の [プログラムの追加と削除] を使用して SBL コンポーネントをアンインストールします。コンピュータをリブートして、再テストします。

ステップ 4　イベント ビューアでユーザの AnyConnect ログをクリアし、再テストします。

ステップ 5　Web をブラウズしてセキュリティ アプライアンスに戻り、AnyConnect を再インストールします。

ステップ 6　1 回リブートします。次回リブート時には、[Start Before Logon] プロンプトが表示されます。

ステップ 7　DART バンドルを収集し、AnyConnect 管理者に送付します。「DART を使用したトラブルシューティング情報の収集」（P.13-4）を参照してください。

ステップ 8　次のエラーが表示された場合は、ユーザの AnyConnect プロファイルを削除します。

```
Description: Unable to parse the profile C:\Documents and Settings\All
Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml.
Host data not available.
```

ステップ 9　.tmpl ファイルに戻って、コピーを .xml ファイルとして保存し、その XML ファイルをデフォルト プロファイルとして使用します。

Windows 7 システムおよび Windows Vista システムでの Start Before Logon（PLAP）の設定

その他の Windows プラットフォームと同じように、Start Before Logon（SBL）機能によって、ユーザが Windows にログインする前に VPN 接続が開始されます。これにより、ユーザは自分のコンピュータにログインする前に、企業のインフラストラクチャに接続されます。Microsoft の Windows 7 および Windows Vista には Windows XP とは異なるメカニズムが使用されているため、Windows 7 および Windows Vista の SBL 機能に使用されているメカニズムも異なります。

SBL AnyConnect 機能は、Pre-Login Access Provider（PLAP）と呼ばれます。これは、接続可能なクレデンシャル プロバイダーです。この機能を使用すると、プログラマチック ネットワーク管理者は、クレデンシャルの収集やネットワーク リソースへの接続など特定のタスクをログイン前に実行することができます。Windows 7 および Windows Vista の SBL 機能は、PLAP により実現されます。PLAP は、vpnplap.dll を使用する 32 ビット版のオペレーティング システムと、vpnplap64.dll を使用する 64 ビット版のオペレーティング システムをサポートしています。PLAP 機能は、x86 および x64 をサポートしています。

（注）　この項では、VPNGINA は Windows XP の Start Before Logon 機能を指し、PLAP は Windows 7 および Windows Vista の Start Before Logon 機能を指します。

PLAP のインストール

vpnplap.dll および vpnplap64.dll の両コンポーネントは、既存の GINA インストール パッケージの一部になっているため、単一のアドオン SBL パッケージをセキュリティ アプライアンスにロードできます。ロードされると、該当するコンポーネントがターゲット プラットフォームにインストールされます。PLAP はオプションの機能です。インストーラ ソフトウェアは、基盤のオペレーティング システムを検出して該当する DLL をシステム ディレクトリに配置します。Windows 7 および Windows Vista よりも前のシステムでは、インストーラにより 32 ビット版のオペレーティング システムに vpngina.dll コンポーネントがインストールされます。Windows 7 または Vista、または Windows Server 2008 では、インストーラは、32 ビット版と 64 ビット版のどちらのオペレーティング システムが使用されているかを判別して、該当する PLAP コンポーネントをインストールします。

（注）　VPNGINA または PLAP コンポーネントがインストールされたまま AnyConnect をアンインストールすると、VPNGINA または PLAP のコンポーネントは無効となり、リモート ユーザの画面に表示されなくなります。

PLAP は、インストールされた後でも、SBL がアクティブ化されるようにユーザ プロファイル <profile.xml> ファイルが変更されるまでアクティブ化されません。「AnyConnect プロファイルでの SBL の有効化」（P.3-15）を参照してください。アクティブ化後に、ユーザは [Switch User] をクリックし、さらに画面下右側の [Network Connect] アイコンをクリックして Network Connect コンポーネントを呼び出します。

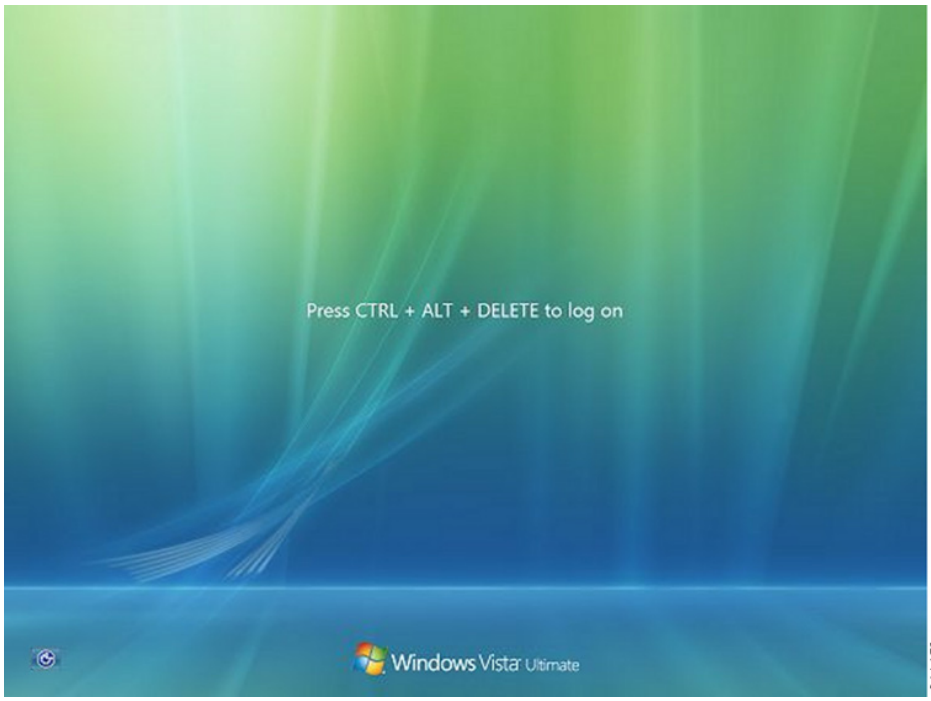
（注）　誤ってユーザ インターフェイスの画面表示を最小化した場合は、**Alt+Tab** キーの組み合わせで元に戻ります。

PLAP を使用した Windows 7 または Windows Vista PC へのログイン

ユーザは、次の手順に従って PLAP を有効にした状態で、Windows 7 または Windows Vista にログインできます。この手順は、Microsoft の要件です。画面の例は、Windows Vista のものです

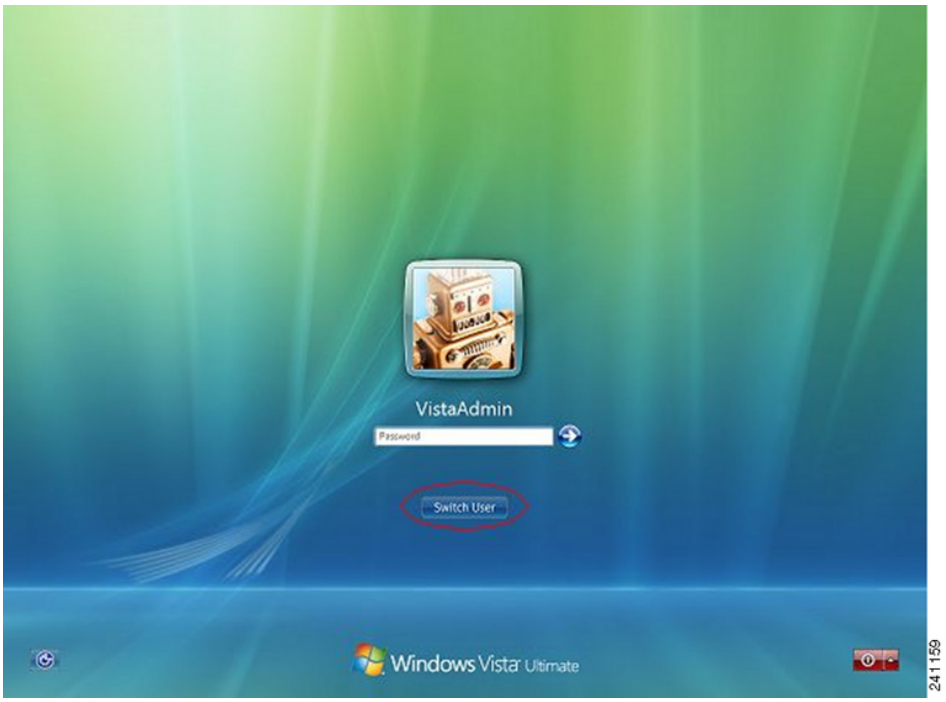
ステップ 1　Windows のスタート画面で、**Ctrl+Alt+Delete** キーの組み合わせを押します（図 3-3）。

図 3-3　[Network Connect] ボタンが表示されたログイン ウィンドウの例



[Switch User] ボタンが表示された Vista のログイン ウィンドウが表示されます。（図 3-4）。

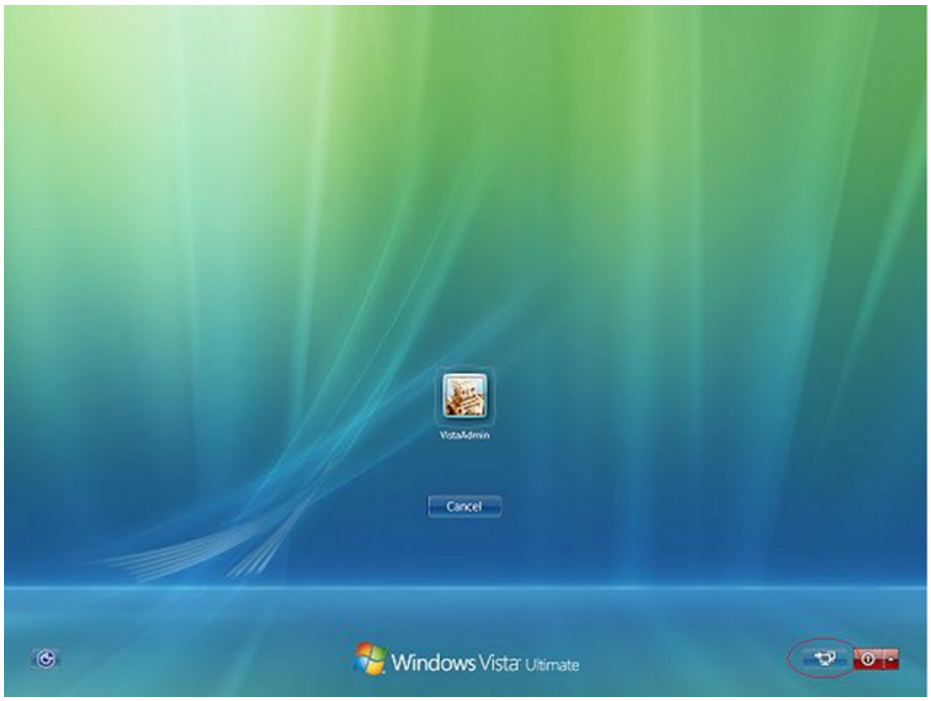
図 3-4　[Switch User] ボタンが表示されたログイン ウィンドウの例



ステップ 2　[Switch User]（図内の赤丸で囲まれているボタン）をクリックします。Vista のネットワーク接続ウィンドウが表示されます。赤丸で囲まれているのは [Network Login] アイコンです。

（注）　AnyConnect 接続によってすでに接続済みのユーザが [Switch User] をクリックしても、VPN 接続は解除されません。[Network Connect] をクリックすると、元の VPN 接続が終了します。[Cancel] をクリックすると、VPN 接続が終了します。

図 3-5　ネットワーク接続ウィンドウの例



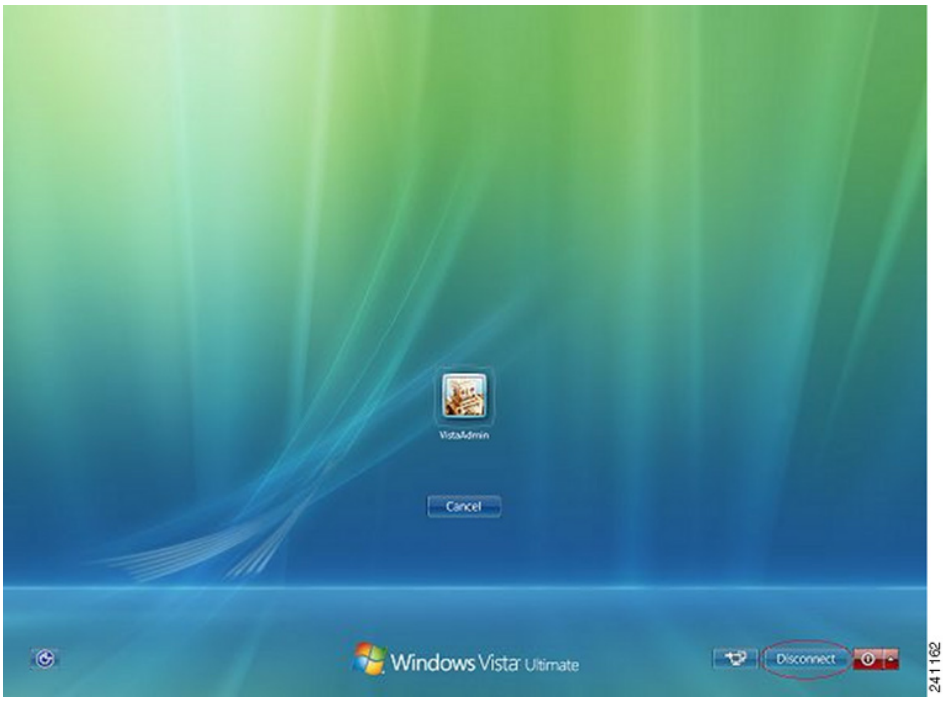
ステップ 3　ウィンドウの右下にある [Network Connect] ボタンをクリックして、AnyConnect を起動します。AnyConnect のログイン ウィンドウが表示されます。

ステップ 4　この GUI を使用して通常どおりログインします。

（注）　この例は、AnyConnect がただ 1 つのインストール済み接続プロバイダーであることを前提としたものです。複数のプロバイダーをインストールしている場合は、このウィンドウに表示される項目の中から、ユーザが使用するものをいずれか 1 つ選択する必要があります。

ステップ 5　接続されると、Vista のネットワーク接続ウィンドウとほぼ同じ画面が表示されます。異なるのは、右下隅に表示されるのが Microsoft の [Disconnect] ボタンである点です（図 3-5）。このボタンは、正常に接続されたことを通知するためだけのものです。

図 3-6　接続解除ウィンドウの例



各ユーザのログイン用アイコンをクリックします。この例では、[VistaAdmin] をクリックするとコンピュータへのログインが完了します。

注意　接続が確立されると、ログイン時間が無制限になります。接続の確立後にユーザがログインを忘れた場合、VPN セッションは無期限に継続されます。

PLAP を使用した AnyConnect からの接続解除

VPN セッションが正常に確立されると、PLAP コンポーネントは元のウィンドウに戻ります。このときウィンドウの右下隅には（図 3-6 で囲まれた）[Disconnect] ボタンが表示されます。

[Disconnect] をクリックすると、VPN トンネルが接続解除されます。

トンネルは、[Disconnect] ボタンの操作によって明示的に接続解除される以外に、次のような状況でも接続解除されます。

- ユーザが PLAP を使用して PC にログインした後で [Cancel] を押した。
- ユーザがシステムへログインする前に PC がシャットダウンした。

この動作は、Windows Vista PLAP アーキテクチャの機能であり、AnyConnect の機能ではありません。

Trusted Network Detection

Trusted Network Detection（TND）を使用すると、ユーザが企業ネットワークの中（*信頼*ネットワーク）にいる場合は AnyConnect により自動的に VPN 接続が解除され、企業ネットワークの外（*非信頼*ネットワーク）にいる場合は自動的に VPN 接続が開始されるようにすることができます。この機能を使用すると、ユーザが信頼ネットワークの外にいるときに VPN 接続を開始することによって、セキュリティ意識を高めることができます。

さらに AnyConnect で Start Before Logon（SBL）が実行されている場合は、ユーザが信頼ネットワークの中に移動した時点で、コンピュータ上に表示されている SBL ウィンドウが自動的に閉じます。

TND を使用している場合でも、ユーザが手動で VPN 接続を確立することは可能です。信頼ネットワークの中でユーザが手動で開始した VPN 接続は解除されません。TND で VPN セッションが接続解除されるのは、最初に非信頼ネットワークにいたユーザが信頼ネットワークに移動した場合だけです。たとえば、ユーザが自宅で VPN 接続を確立した後で会社に移動すると、この VPN セッションは TND によって接続解除されます。

TND 機能では AnyConnect の GUI を制御することで接続が自動的に開始されるため、GUI を常に実行している必要があります。ユーザが GUI を終了した場合、TND によって VPN 接続が自動的に開始されることはありません。

TND は AnyConnect VPN Client プロファイルに設定します。ASA の設定を変更する必要はありません。

Trusted Network Detection の要件

Trusted Network Detection（TND）は、この AnyConnect リリースでサポートされた Microsoft Windows および Mac OS X オペレーティング システムを動作しているコンピュータでサポートされています。

常時接続が設定されている、またはされていない Trusted Network Detection は、IPv4 ネットワークおよび IPv6 ネットワークで ASA に接続された IPv6 および IPv4 の VPN 接続でサポートされています。

Trusted Network Detection の設定

クライアント プロファイルで TND の設定を行う手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Preferences (Part 2)] ペインに移動します。

ステップ 3　[Automatic VPN Policy] をオンにします。

（注）　[Automatic VPN Policy] の設定にかかわらず、ユーザは VPN 接続を手動で制御できます。

ステップ 4　ユーザが企業ネットワークの中（信頼ネットワーク）にいる場合のクライアントの動作を規定する信頼ネットワーク ポリシーを選択します。次のオプションがあります。

- [Disconnect]：信頼ネットワークではクライアントにより VPN 接続が終了します。
- [Connect]：信頼ネットワークではクライアントにより VPN 接続が開始されます。
- [Do Nothing]：信頼ネットワークではクライアントの動作はありません。[Trusted Network Policy] および [Untrusted Network Policy] を共に [Do Nothing] に設定すると、Trusted Network Detection（TND）は無効となります。
- [Pause]：ユーザが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、AnyConnect は VPN セッションを（接続解除ではなく）一時停止します。ユーザが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。

ステップ 5　ユーザが企業ネットワークの外にいる場合のクライアントの動作を規定する非信頼ネットワーク ポリシーを選択します。次のオプションがあります。

- [Connect]：非信頼ネットワークが検出されるとクライアントにより VPN 接続が開始されます。
- [Do Nothing]：非信頼ネットワークが検出されるとクライアントにより VPN 接続が開始されます。このオプションを選択すると、VPN 常時接続は無効となります。[Trusted Network Policy] および [Untrusted Network Policy] を共に [*Do Nothing*] に設定すると、Trusted Network Detection は無効となります。

ステップ 6　Trusted DNS Domains（クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列））を指定します。*.cisco.com などがこれに該当します。DNS サフィックスでは、ワイルドカード（*）がサポートされます。DNS サフィックスの照合の例については、表 3-1 を参照してください。

ステップ 7　信頼 DNS サーバを指定します。ここでは、クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができるすべての DNS サーバ アドレス（カンマ区切りの文字列）を指定します。たとえば、203.0.113.1,2001:DB8::1 です。DNS サーバ アドレスでは、ワイルドカード（*）はサポートされていません。

（注）　TND を機能させるためには、すべての DNS サーバを指定する必要があります。TrustedDNSDomains と TrustedDNSServers の両方を設定した場合は、セッションが両方の設定に一致していないと、信頼ネットワークの中にあると見なされません。

表 3-1　DNS サフィックスの一致の例

照合する DNS サフィックス	TrustedDNSDomains に使用する値
example.com（のみ）	example.com
example.com および anyconnect.cisco.com	*.example.com または example.com, anyconnect.example.com
asa.example.com および example.cisco.com	*.example.com または asa.example.com, anyconnect.example.com

TND と複数のプロファイルで複数のセキュリティ アプライアンスに接続するユーザ

ユーザのコンピュータ上に複数のプロファイルがあると、ユーザが TND の有効なセキュリティ アプライアンスから TND が有効でないセキュリティ アプライアンスへ接続を変更する際に問題が発生することがあります。ユーザが TND の有効なセキュリティ アプライアンスに接続していた場合、そのユーザは TND が有効なプロファイルを受け取っています。そのユーザが、信頼ネットワークの外でコンピュータをリブートすると、TND が有効であるクライアントの GUI が表示され、最後に接続していたセキュリティ アプライアンスへの接続が試行されますが、このセキュリティ アプライアンスでは、TND が有効でない可能性があります。

クライアントが TND の有効なセキュリティ アプライアンスに接続している場合、ユーザが TND の有効でない ASA に接続するためには、手動で接続解除してから、TND の有効でないセキュリティ アプライアンスに接続する必要があります。ユーザが TND の有効なセキュリティ アプライアンスと TND が有効でないセキュリティ アプライアンスのどちらにも接続する可能性がある場合は、TND を有効にする前にこの問題を考慮してください。

この問題を回避する手段としては、次のような対策が考えられます。

- 企業ネットワーク上にある*すべての ASA* にロードされるクライアント プロファイルで、TND を有効にする。
- すべての ASA がリストされた *1 つのプロファイル*をホスト エントリ セクションに作成し、このプロファイルを*すべての* ASA にロードする。
- 複数の異なるプロファイルが必要ない場合は、*すべての* ASA のプロファイルに同じプロファイル名を使用する。既存のプロファイルは各 ASA により上書きされます。

VPN 常時接続

ユーザがコンピュータにログインすると VPN セッションが自動的に確立されるように AnyConnect の設定を行うことができます。VPN セッションは、ユーザがコンピュータからログアウトするか、セッション タイマーまたはアイドル セッション タイマーが期限に達するまでは開いた状態が維持されます。これらのタイマーの値は、セッションに割り当てられたグループ ポリシーに指定されます。AnyConnect と ASA の接続が解除されても、このいずれかのタイマーが期限に達しない限り、ASA およびクライアントではセッションに割り当てられたリソースが保持されます。AnyConnect では、セッションが開いている場合は、それを再アクティブ化するために接続の再確立が継続して試行され、セッ

ションが開いていない場合は、新しい VPN セッションの確立が継続的に試行されます。

（注） 常時接続がオンであっても、ユーザがログインしていない場合は、AnyConnect は VPN 接続を確立しません。AnyConnect が VPN 接続を確立するのは、ログイン後に限られます。

*（ログイン後の）VPN 常時接続*では、コンピュータが信頼ネットワーク内に存在しない場合にはインターネット リソースへのアクセスを制限することによってセキュリティ上の脅威からコンピュータを保護するという企業ポリシーが適用されます。

注意 VPN 常時接続では、プロキシを介した接続はサポートされていません。

AnyConnect では、プロファイルで VPN 常時接続が検出されると、エンドポイントを保護するためにその他の AnyConnect プロファイルがすべて削除され、ASA に接続するよう設定されたパブリック プロキシはいずれも無視されます。

脅威に対する保護を強化するためにも、VPN 常時接続の設定を行う場合は、次のような追加的な保護対策を講じることを推奨します。

- VPN 常時接続が設定されたプロファイルをエンドポイントに事前に展開し、事前定義された ASA への接続を制限します。事前展開により、不正なサーバへのアクセスを防止することができます。
- ユーザが処理を終了できないように管理者権限を制限します。管理者権限を持つ PC ユーザは、エージェントを停止することにより VPN 常時接続ポリシーを無視することができます。VPN 常時接続の安全性を十分に確保する必要がある場合は、ユーザに対してローカル管理者権限を付与しないでください。
- Windows コンピュータ上で次のフォルダまたはシスコ サブフォルダへのアクセスを制限します。
  - Windows XP ユーザの場合：C:\Document and Settings\All Users
  - Windows Vista ユーザおよび Windows 7 ユーザの場合：C:\ProgramData

  限定的な権限または標準的な権限を持つユーザは、それぞれのプログラム データ フォルダに対して書き込みアクセスを実行できる場合があります。このアクセスを使用すれば、AnyConnect プロファイル ファイルを削除できるため、常時接続機能を無効にすることができます。
- Windows ユーザのグループ ポリシー オブジェクト（GPO）を事前に展開して、限定的な権限を持つユーザが GUI を終了できないようにします。Mac OS ユーザに対してもこれに相当するものを事前に展開します。

VPN 常時接続の要件

VPN 常時接続をサポートするためには、次のライセンスのうちいずれか 1 つが必要です。

- AnyConnect Premium（SSL VPN Edition）
- Cisco AnyConnect セキュア モビリティ

  Cisco AnyConnect セキュア モビリティ ライセンスを、AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのどちらかと組み合わせて使用することにより VPN 常時接続をサポートできます。

VPN 常時接続を使用するには、ASA 上に有効なサーバ証明書が設定されている必要があります。設定されていない場合、VPN 常時接続は失敗し、その証明書が無効であることを示すイベントがログに記録されます。

VPN 常時接続を設定する場合は、ご使用のサーバ証明書がストリクト モードに合格できることを確認してください。

VPN 常時接続は、このリリースでサポートされている Microsoft Windows および Mac OS X オペレーティング システムを実行するコンピュータをサポートしています。

不正なサーバへの VPN 接続をロックする VPN 常時接続プロファイルをダウンロードできないようにするため、AnyConnect クライアントでは、セキュア ゲートウェイに接続する際、有効で信頼できるサーバ証明書が必要となります。

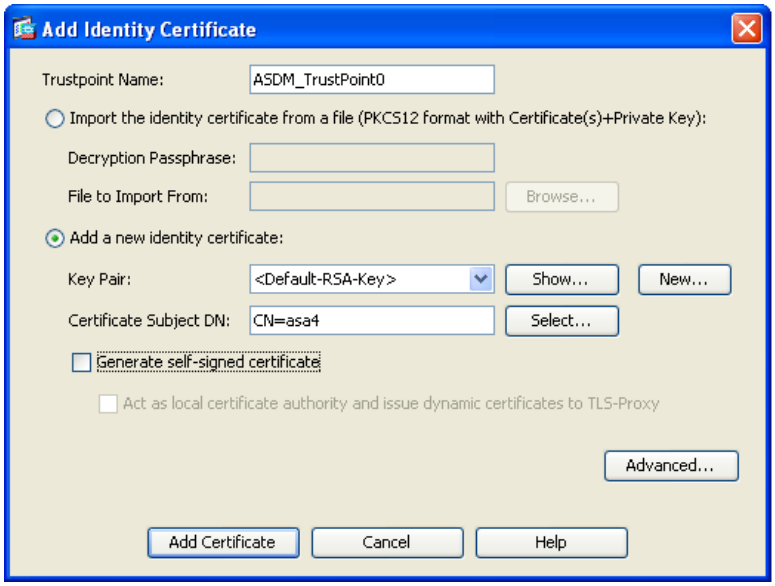
ヒント　認証局（CA）からデジタル証明書を購入し、それをセキュア ゲートウェイ上に登録することを強く推奨します。

自己署名証明書を生成すると、接続するユーザには証明書の警告が表示されます。この場合は、その証明書を信頼するようにブラウザを設定すると、それ以降は警告が表示されないようにすることができます。

（注）　自己署名証明書の使用はお勧めしません。理由は、ユーザが誤って不正なサーバ上の証明書を信頼するようにブラウザを設定する可能性があるため、また、ユーザがセキュア ゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。

ASDM では、ASA 上でのこの問題を解決できるよう、[Identity Certificates] パネル（[Configuration] > [Remote Access VPN] > [Certificate Management] > [Identity Certificates]）に、公開証明書を容易に登録するための [Enroll ASA SSL VPN with Entrust] ボタンが用意されています。このパネルにある [Add] ボタンを使用すると、ファイルから公開証明書をインポートするか、または自己署名証明書を生成できます。

図 3-7　[Add Identity Certificate] ダイアログ

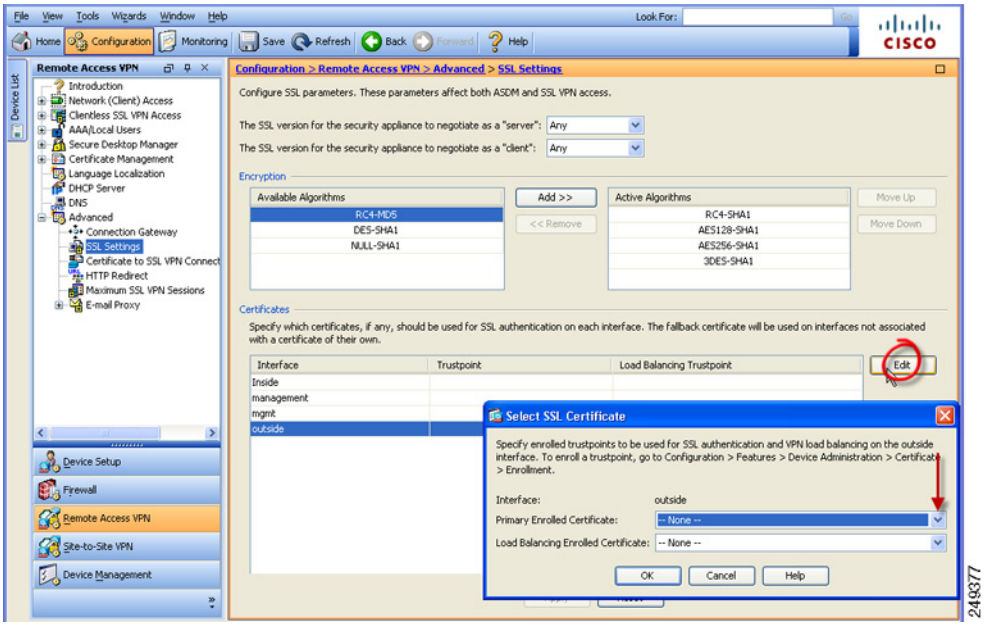


（注）　これらの手順は、証明書の設定に関するガイドラインとして記載されたものです。詳細については、ASDM の [Help] ボタンをクリックするか、設定するセキュア ゲートウェイ用の ASDM または CLI ガイドを参照してください。

自己署名インターフェイスを生成する場合は、[Advanced] ボタンを使用して、outside インターフェイスのドメイン名および IP アドレスを指定します。

証明書を登録したら、それを outside インターフェイスに割り当てます。その手順として、[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings] を選択し、[Certificates] エリアで「outside」エントリを編集して、[Primary Enrolled Certificate] ドロップダウン リストから証明書を選択します。

図 3-8　outside インターフェイスへの証明書の割り当て（画面は ASDM 6.3）



すべてのセキュア ゲートウェイに証明書を追加し、それを outside インターフェイスの IP アドレスに関連付けます。

サーバ リストへのロードバランシング バックアップ クラスタ メンバーの追加

VPN 常時接続は、AnyConnect VPN セッションのロード バランシングに影響を与えます。VPN 常時接続を無効にした状態では、クライアントからロードバランシング クラスタ内のマスター デバイスに接続すると、クライアントはマスター デバイスから任意のバックアップ クラスタ メンバーにリダイレクトされます。VPN 常時接続を有効にすると、クライアント プロファイルのサーバ リスト内にバックアップ クラスタ メンバーのアドレスが指定されていない限り、クライアントがマスター デバイスからリダイレクトされることはありません。このため、サーバ リストにはいずれかのバックアップ クラスタ メンバーを必ず追加するようにしてください。

クライアント プロファイルにバックアップ クラスタ メンバーのアドレスを指定する場合は、ASDM を使用してロードバランシング バックアップ サーバ リストを追加します。手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Server List] ペインに移動します。

ステップ 3　ロードバランシング クラスタのマスター デバイスであるサーバを選択して、[Edit] をクリックします。

ステップ 4　いずれかのロードバランシング クラスタ メンバーの FQDN または IP アドレスを入力します。

VPN 常時接続の設定

コンピュータが非信頼ネットワーク内に存在することが検知された場合に限って VPN セッションが自動的に確立されるよう AnyConnect を設定する手順は次のとおりです。

ステップ 1　TND を設定します（「Trusted Network Detection の設定」（P.3-21）を参照）。

ステップ 2　[Always On] をオンにします。

VPN 常時接続からユーザを除外するポリシーの設定

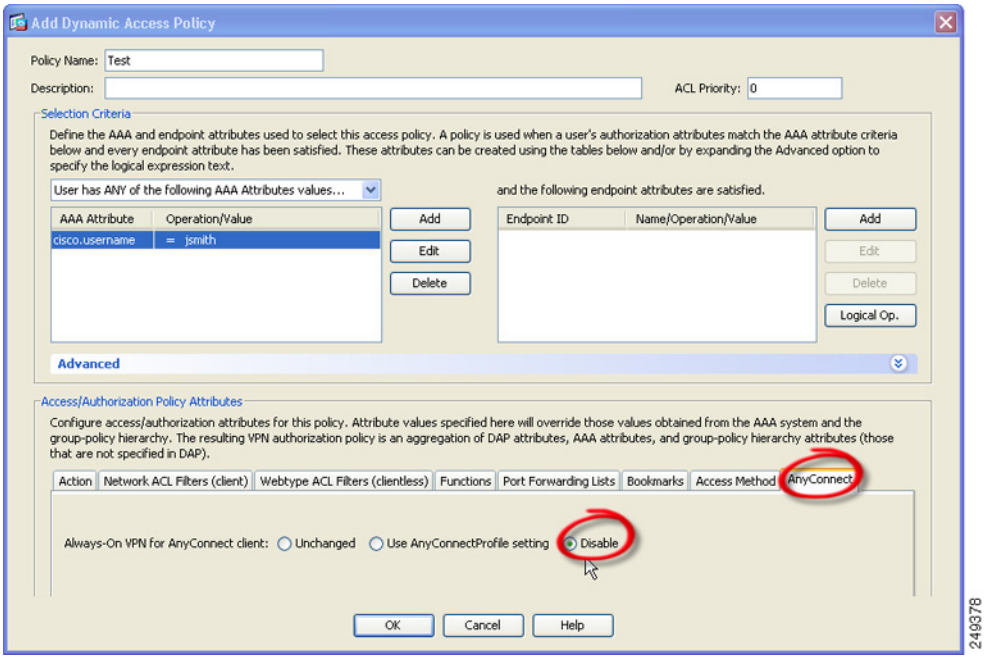
VPN 常時接続は、デフォルトでは無効になっています。常時接続ポリシーに優先して適用される除外規定を設定することができます。たとえば、特定のユーザに対して他社との VPN セッションを確立できるようにしつつ、企業外資産に対しては VPN 常時接続ポリシーを除外するという場合があります。

グループ ポリシーおよびダイナミック アクセス ポリシーで VPN 常時接続パラメータを設定すると、常時接続ポリシーを上書きすることができます。これにより、ポリシーの割り当てに使用される一致基準に従って例外を指定できます。AnyConnect ポリシーでは VPN 常時接続が有効になっているが、ダイナミック アクセス ポリシーまたはグループ ポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループ ポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。

次に、AAA またはエンドポイント条件を使用して企業外資産へのセッションを照合するダイナミック アクセス ポリシーを設定する手順を示します。

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

図 3-9　VPN 常時接続からのユーザの除外



ステップ 2　ユーザを VPN 常時接続から除外する条件を設定します。たとえば、[Selection Criteria] エリアを使用して、ユーザのログイン ID に一致する AAA 属性を指定します。

ステップ 3　[Add Dynamic Access Policy] ウィンドウまたは [Edit Dynamic Access Policy] ウィンドウの下半分にある [AnyConnect] タブをクリックします。

ステップ 4　[Always-On VPN for AnyConnect client] の横にある [Disable] をクリックします。

Cisco AnyConnect Secure Mobility Client ポリシーでは VPN 常時接続が有効になっているが、ダイナミック アクセス ポリシーまたはグループ ポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループ ポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。

VPN 常時接続用の [Disconnect] ボタン

AnyConnect は、VPN 常時接続セッション用の [Disconnect] ボタンをサポートしています。これを有効にすると、AnyConnect では VPN セッションが確立された時点で [Disconnect] ボタンが表示されます。VPN 常時接続セッションのユーザは、[Disconnect] をクリックすることが必要になる場合があるため、次のような問題に対処できるよう代替セキュア ゲートウェイを選択することができます。

- 現在の VPN セッションに関するパフォーマンスの問題。

- VPN セッションが中断した後に生じる再接続の問題。

[Disconnect] ボタンをクリックすると、すべてのインターフェイスがロックされます。これにより、データの漏洩を防ぐことができるほか、VPN セッションの確立には必要のないインターネット アクセスからコンピュータを保護することができます。

注意　[Disconnect] ボタンを無効にすると、VPN アクセスが妨害または阻止されることがあります。

VPN 常時接続セッション中にユーザが [Disconnect] ボタンをクリックすると、AnyConnect ではすべてのインターフェイスがロックされます。これにより、データの漏洩を防ぐことができるほか、VPN セッションの確立には必要のないインターネット アクセスからコンピュータを保護することができます。AnyConnect では、接続障害ポリシーの内容にかかわらず、すべてのインターフェイスがロックされます。

注意　[Disconnect] ボタンをクリックすると、すべてのインターフェイスがロックされます。これにより、データの漏洩を防ぐことができるほか、VPN セッションの確立には必要のないインターネット アクセスからコンピュータを保護することができます。上述した理由により、[Disconnect] ボタンを無効にすると、VPN アクセスが妨害または阻止されることがあります。

[Disconnect] ボタンに関する要件

VPN 常時接続用の接続解除オプションに関する要件は、「VPN 常時接続の要件」（P.3-24）と同じです。

[Disconnect] ボタンの有効化 / 無効化

VPN 常時接続を有効すると、プロファイル エディタでは、[Disconnect] ボタンがデフォルトで有効になります。[Disconnect] ボタンの設定を表示および変更する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Preferences (Part 2)] ペインに移動します。

ステップ 3　[Allow VPN Disconnect] をオンまたはオフにします。

VPN 常時接続に関する接続障害ポリシー

接続障害ポリシーでは、VPN 常時接続が有効であり、かつ AnyConnect で VPN セッションが確立できない場合（セキュア ゲートウェイが到達不能の場合など）に、コンピュータからインターネットにアクセスできるようにするかどうかを指定します。フェール クローズド ポリシーでは、VPN アクセスを除くネットワーク接続が無効になります。フェール オープン ポリシーでは、ネットワーク接続が許可

されます。AnyConnect では、接続障害ポリシーの内容にかかわらず、VPN 接続の確立が継続的に試行されます。次の表は、フェール オープン ポリシーおよびフェール クローズド ポリシーに関する説明をまとめたものです。

VPN 常時接続ポリシー	シナリオ	メリット	トレードオフ
フェール オープン	AnyConnect が VPN セッションの確立または再確立に失敗しました。この障害は、セキュア ゲートウェイが使用できない場合、または AnyConnect で（空港、喫茶店、ホテルなどで使用されることの多い）キャプティブ ポータルの存在を検出できない場合に発生することがあります。	最大限のネットワーク アクセス権を付与することで、インターネット リソースを始めとするローカル ネットワーク リソースへのアクセスが必要なタスクをユーザが継続的に実行できるようにします。	VPN セッションが確立されるまで、セキュリティや保護の対策は実行できません。そのため、エンドポイント デバイスが Web ベースのマルウェアに感染する可能性があるほか、機密データが漏洩する可能性もあります。
フェール クローズ	このオプションは主に、ネットワーク アクセスが常時利用できることよりもセキュリティの永続性の方が重視される、安全意識のきわめて高い組織に適しています。この点を除けば上記と同じです。	スプリット トンネリングにより許可されるプリンタやテザー デバイスといったローカル リソースへのアクセスを除くすべてのネットワーク アクセスが制限されます。テザー デバイスへのアクセスを除くすべてのネットワーク アクセスが制限されるため、エンドポイントは Web ベースのマルウェアから保護され、機密データの漏洩も常時防ぐことができます。	このオプションを選択した場合、VPN セッションが確立されるまでは、プリンタやテザー デバイスといったローカル リソースへのアクセスを除くすべてのネットワーク アクセスが制限されます。そのため、ユーザが VPN 外部のインターネット アクセスを要求したにもかかわらずセキュア ゲートウェイにアクセスできない場合には、生産性が著しく低下します。

注意　AnyConnect が VPN セッションの確立に失敗した場合は、接続障害クローズド ポリシーによりネットワーク アクセスは制限されます。AnyConnect では、「キャプティブ ポータル ホットスポットの検出と修復」（P.3-32）で説明されているキャプティブ ポータルの大半が検出されます。ただし、キャプティブ ポータルを検出できない場合は、接続障害クローズド ポリシーによりすべてのネットワーク接続が制限されます。接続障害クローズド ポリシーは、細心の注意を払って実装してください。

クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープン ポリシーを使用して VPN 常時接続を展開し、ユーザを通じて AnyConnect がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズド ポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズド ポリシーを展開する場合は必ず、VPN ユーザに対して接続障害クローズド ポリシーのメリットだけでなく、ネットワーク アクセスの制限についても周知してください。

接続障害ポリシーに関する要件

接続障害ポリシー機能をサポートするためには、次のライセンスのうちいずれか 1 つが必要です。

- AnyConnect Premium（SSL VPN Edition）
- Cisco AnyConnect セキュア モビリティ

  Cisco AnyConnect セキュア モビリティ ライセンスを、AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのどちらかと組み合わせて使用することにより、接続障害ポリシーをサポートできます。

接続障害ポリシーは、Microsoft Windows 7、Vista、XP、および Mac OS X 10.6、10.7 が実行されているコンピュータのみサポートしています。

接続障害ポリシーの設定

接続障害ポリシーのデフォルト設定では、VPN 常時接続が設定され、かつ VPN が到達不能の場合、インターネット アクセスが制限されます。接続障害ポリシーの設定を行う手順は次のとおりです。

ステップ 1　TND を設定します（「Trusted Network Detection の設定」（P.3-21）を参照）。

ステップ 2　[Always On] をオンにします。

ステップ 3　[Connect Failure Policy] パラメータを次のいずれかに設定します。

- [Closed]：（デフォルト）セキュア ゲートウェイが到達不能の場合は、インターネット アクセスが制限されます。AnyConnect では、コンピュータが接続を許可されているセキュア ゲートウェイにバインドされていない、エンドポイントからのトラフィックをすべてブロックするパケット フィルタを有効にすることで、この制限が実現されています。

  キャプティブ ポータル修復（次の項で説明）は、ポリシーの一部として特に有効にされていない限り、フェールクローズド ポリシーでは制限されます。クライアント プロファイルで [Apply Last VPN Local Resources] が有効になっている場合、制限された状態では、直近の VPN セッションにより適用されたローカル リソース ルールを適用することができます。たとえば、これらのルールにより、アクティブ シンクやローカル印刷へのアクセスを規定することができます。常時接続が有効な場合は、AnyConnect ソフトウェアのアップグレード中、ネットワークはブロックされずオープンの状態になります。[Closed] 設定の目的は、エンドポイントを保護するプライベート ネットワーク内のリソースが使用できない場合に、企業の資産をネットワークに対する脅威から保護することにあります。
- [Open]：この設定では、クライアントが ASA に接続できない場合、ブラウザなどのアプリケーションによるネットワーク アクセスが許可されます。[Disconnect] ボタンが有効で、かつユーザが [Disconnect] をクリックした場合は、オープン接続障害ポリシーは適用されません。

キャプティブ ポータル ホットスポットの検出と修復

空港、喫茶店、ホテルなど、Wi-Fi や有線アクセスを提供している施設では、アクセスする前に料金を支払ったり、アクセプタブル ユース ポリシーを順守することに同意したりする必要があります。こうした施設では、*キャプティブ ポータル*と呼ばれる技術を使用することにより、ユーザがブラウザを開いてアクセス条件に同意するまではアプリケーションの接続が行えないようにしています。

ここでは、キャプティブ ポータル ホットスポットの検出機能および修復機能について説明します。

キャプティブ ポータルの修復に関する要件

キャプティブ ポータルの検出と修復をどちらもサポートするためには、次のライセンスのうちいずれか 1 つが必要です。

- AnyConnect Premium（SSL VPN Edition）
- Cisco AnyConnect セキュア モビリティ

  Cisco AnyConnect セキュア モビリティ ライセンスを、AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのどちらかと組み合わせて使用することにより、キャプティブ ポータルの検出および修復をサポートできます。

キャプティブ ポータルの検出と修復は、AnyConnect のこのリリースでサポートされている Microsoft Windows および Mac OS X オペレーティング システムでサポートされています。

キャプティブ ポータル ホットスポットの検出

AnyConnect では、接続ができない場合、その原因を問わず GUI に「Unable to contact *VPN server*」というメッセージが表示されます。*VPN server* は、セキュア ゲートウェイを表します。常時接続が有効であり、かつキャプティブ ポータルが存在しない場合、クライアントでは VPN への接続が継続的に試行され、それによってステータス メッセージが更新されます。

VPN 常時接続が有効であり、接続障害ポリシーがクローズで、かつキャプティブ ポータルの修復が無効の場合に、AnyConnect でキャプティブ ポータルの存在が検出されると、AnyConnect の GUI には接続および再接続のたびに次のようなメッセージが表示されます。

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

AnyConnect によりキャプティブ ポータルの存在が検出され、かつ AnyConnect の設定が上述した内容と異なる場合、AnyConnect の GUI には接続および再接続のたびに次のようなメッセージが表示されます。

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

キャプティブ ポータルの検出はデフォルトで有効になっており、設定を行うことはできません。

キャプティブ ポータル検出中は、AnyConnect によりブラウザの設定が変更されることはありません。

キャプティブ ポータル ホットスポット修復

*キャプティブ ポータルの修復*は、ネットワーク アクセス権を取得できるように、キャプティブ ポータルのホット スポット要件を満たすためのプロセスです。

キャプティブ ポータルの修復は、AnyConnect により実行されるものではなく、エンド ユーザによる修復の実行に依存しています。

エンド ユーザは、ホットスポット プロバイダーの要件を満たすことで、キャプティブ ポータル修復を実行します。これらの要件には、ネットワークにアクセスするための料金の支払い、アクセプタブル ユース ポリシーへの署名、その両方、またはプロバイダーが定義するその他の要件などがあります。

AnyConnect の常時接続が有効になっており、接続障害ポリシーが [Closed] に設定されている場合は、AnyConnect VPN Client プロファイルで、キャプティブ ポータル修復を明示的に許可する必要があります。常時接続が有効になっており、接続障害ポリシーが [Open] に設定されている場合は、ユーザはネットワークへのアクセスを制限されることはないため、AnyConnect VPN Client プロファイルでキャプティブ ポータル修復を明示的に許可する必要はありません。

キャプティブ ポータル ホットスポット修復をサポートするための設定

常時接続機能が有効になっており、接続障害ポリシーがクローズドに設定されている場合は、AnyConnect VPN クライアント ポリシーでキャプティブ ポータル修復を有効にする必要があります。接続障害ポリシーがオープンに設定されている場合は、ユーザがネットワーク アクセスを制限されることがないため、AnyConnect VPN クライアント ポリシーでその他の設定を行わなくても、キャプティブ ポータルを修復できます。

デフォルトの場合、キャプティブ ポータルの修復は無効です。キャプティブ ポータル修復を有効にするには、次の作業を実行します。

ステップ 1　接続障害ポリシーの設定を行います（「接続障害ポリシーの設定」（P.3-31）を参照）。

ステップ 2　接続障害ポリシーをクローズドに設定した場合は、次のパラメータを設定します。

- Allow Captive Portal Remediation：オンにすると、クローズ接続障害ポリシーにより適用されたネットワーク アクセスの制限が Cisco AnyConnect Secure Mobility Client により解除されます。デフォルトの場合、このパラメータはオフになっており、セキュリティは最高度に設定されます。ただし、クライアントから VPN へ接続する必要があるにもかかわらず、キャプティブ ポータルによりそれが制限されている場合は、このパラメータをオンにする必要があります。
- Remediation Timeout：AnyConnect によりネットワーク アクセス制限が解除される時間を分単位で入力します。ユーザには、キャプティブ ポータルの要件を満たすことができるだけの十分な時間が必要です。

  VPN 常時接続が有効な場合に、ユーザが [Connect] をクリックするか、または再接続が実行されると、キャプティブ ポータルが存在することを示すメッセージ ウィンドウが表示されます。この時点でユーザは、Web ブラウザ ウィンドウを開いてキャプティブ ポータルを修復することができます。

ユーザがキャプティブ ポータル ページにアクセスできない場合

ユーザがキャプティブ ポータル修復ページにアクセスできない場合は、修復できるようになるまで次の手順を試行するようユーザに指示してください。

ステップ 1　ネットワーク インターフェイスを無効にした後、再度有効にします。この操作により、キャプティブ ポータルの検出が再試行されます。

ステップ 2　修復を実行するためのブラウザを 1 つだけ残し、インスタント メッセージング プログラム、電子メール クライアント、IP Phone クライアントなど、HTTP を使用するその他のアプリケーションをすべて終了します。キャプティブ ポータルは、接続の反復試行を無視し、結果的にクライアント側でタイムアウトにすることで、DoS 攻撃を積極的に阻止することができます。HTTP 接続が多数のアプリケーションによって試行された場合、この問題の深刻度は大きくなります。

ステップ 3　ステップ 1 を再試行します。

ステップ 4　コンピュータをリスタートします。

キャプティブ ポータルの検出の失敗

次のような状況では、誤ってキャプティブ ポータルと見なされる場合があります。

- AnyConnect が、サーバ名が正しくない証明書（CN）を持った ASA に接続しようとしている場合、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。

  これを回避するには、ASA 証明書が正しく設定されていることを確認します。証明書の CN 値は、VPN クライアント プロファイルの ASA サーバの名前と一致する必要があります。

- ASA の前に別のデバイスがネットワーク上に存在し、そのデバイスが ASA への HTTPS アクセスをブロックして、クライアントによる ASA への接続に応答すると、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。これは、ユーザが内部ネットワークに存在し、ファイアウォールを介して ASA に接続している場合に発生する可能性があります。

  企業内から ASA へのアクセスを制限する必要がある場合、ASA のアドレスへの HTTP および HTTPS トラフィックが HTTP ステータスを返さないようにファイアウォールを設定します。ASA への HTTP/HTTPS アクセスは許可するか、完全にブロック（ブラック ホールとも呼ばれます）し、ASA に送信された HTTP/HTTPS 要求が予期しない応答を返さないようにします。

ローカル プリンタおよびテザー デバイスをサポートしたクライアント ファイアウォール

ユーザが ASA に接続すると、すべてのトラフィックがその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。ASA を使用してエンドポイントの OS のファイアウォール機能を導入することにより、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ことができます。

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。

クライアント ファイアウォール機能は、このリリースでサポートされている Windows、Mac OS X、および Linux オペレーティング システムでサポートされています。

（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導入」（P.3-36）
- 「テザー デバイスのサポート」（P.3-37）

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導入

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ています。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。

表 3-2 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。

表 3-2　送信元ポート / 宛先ポートと影響を受けるトラフィックの方向

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

表 3-3 は、ローカル印刷に関する ACL ルールの例です。

表 3-3　ローカル印刷に関する ACL ルールの例

説明	権限	インターフェイス	プロトコル	送信元ポート	宛先アドレス	宛先ポート
すべて拒否	拒否	パブリック	任意	デフォルト[1]	任意	デフォルト
LPD	許可	パブリック	TCP	デフォルト	任意	515

表 3-3　ローカル印刷に関する ACL ルールの例 （続き）

説明	権限	インターフェイス	プロトコル	送信元ポート	宛先アドレス	宛先ポート
IPP	許可	パブリック	TCP	デフォルト	任意	631
プリンタ	許可	パブリック	TCP	デフォルト	任意	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	任意	137
NetBios	許可	パブリック	UDP	デフォルト	任意	137

1. 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。

ローカル印刷サポートの設定

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。[Edit Internal Group Policy] ウィンドウが表示されます。

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　表 3-3 にあるルールを使用して、ACL を作成し ACE を指定します。この ACL をパブリック 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 エディタで [Preferences (Cont)] に移動し、[Apply last local VPN resource rules] をオンにするとファイアウォール ルールを適用することができます。

テザー デバイスのサポート

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

手順は次のとおりです。

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。[ACL Manager] が表示されます。

ステップ 3　[Extended ACL] タブをクリックします。

ステップ 4　[Add] をクリックし、さらに [Add ACL] をクリックします。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。[Edit ACE] ウィンドウが表示されます。

ステップ 6　[Action] で [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。

Mac OS X の新規インストール ディレクトリ構造

AnyConnect の以前のリリースでは、AnyConnect コンポーネントは **opt/cisco/vpn** のパスにインストールされました。リリース 3.0.4 以降では、AnyConnect コンポーネントは **/opt/cisco/anyconnect** パスにインストールされています。

Web セキュリティ クライアント プロファイルの ScanCenter ホステッド コンフィギュレーション サポート

Web セキュリティ ホステッド クライアント プロファイルの ScanCenter ホステッド コンフィギュレーションを使用すると、管理者は Web セキュリティ クライアントに新しい Web セキュリティ クライアント プロファイルを提供できます。Web セキュリティを備えたデバイスは、クラウドから新しいクライアント プロファイルをダウンロードできます（ホステッド コンフィギュレーション ファイルは ScanCenter サーバに格納されています）。この機能の唯一の前提条件は、有効なクライアント プロファイルでデバイスに Web セキュリティがインストールされていることです。

管理者は、Web セキュリティ プロファイル エディタを使用してクライアント プロファイルを作成してから、クリア テキスト XML ファイルを ScanCenter サーバにアップロードします。この XML ファイルには、ScanSafe からの有効なライセンス キーが含まれている必要があります。ホステッド コンフィギュレーション機能では、ホステッド コンフィギュレーション（ScanCenter）サーバから新しいクライアント プロファイル ファイルを取得する際にライセンス キーが使用されます。新しいクライアント プロファイル ファイルがサーバ上に置かれたら、Web セキュリティを実装したデバイスは自動的にサーバをポーリングし、新しいクライアント プロファイルをダウンロードします。これには、既存の Web セキュリティ クライアント プロファイルにあるライセンスがホステッド サーバ上のクライアント プロファイルに関連付けられたライセンスと同じであることが条件となります。いったん新しいクライアント プロファイルがダウンロードされたら、管理者が新しいクライアント プロファイル ファイルを使用可能にするまで、Web セキュリティにより同じファイルが再度ダウンロードされることはありません。

（注） ホステッド コンフィギュレーション機能を使用するためには、ScanSafe ライセンス キーが含まれた有効なクライアント プロファイル ファイルを使用して、Web セキュリティ クライアント デバイスをあらかじめインストールしておく必要があります。

スプリット トンネリングの設定

スプリット トンネリングにより、VPN トンネル経由（暗号化されている）でエンドポイントから ASA へネットワーク トラフィックをルーティングし、VPN トンネル外（暗号化されていない、つまりクリア テキスト）のエンドポイントからその他のネットワーク トラフィックをルーティングできます。

ユニファイド アクセス コントロール リストを作成し、そのリストを VPN トンネルに組み込むよう要求する、または VPN トンネルから除外するよう要求することで、スプリット トンネリングを実装します。ユニファイド 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。

スプリット トンネリングは、ASA のネットワーク（クライアント）アクセス内部グループ ポリシーで設定されています。

AnyConnect クライアントおよびレガシー Cisco VPN クライアント（IPsec/IKEv1 クライアント）は、ASA によってクライアントに割り当てられた IP アドレスと同じサブネット内のサイトにトラフィックを渡す場合、動作が異なります。AnyConnect では、クライアントは、設定済みのスプリット 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含まれるすべてのサイトにトラフィックを渡します。たとえば、ASA によってクライアントに割り当てられた 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。レガシー Cisco VPN Client は、ASA によってクライアントに割り当てられたサブネットに関係なく、スプリット トンネリング ポリシーで指定されたアドレスだけにトラフィックを渡します。

したがって、スプリット トンネル IPv4 または IPv6 ポリシーで定義されたユニファイド アクセス コントロール リストでは、予想されたローカル サブネットを正しく参照する割り当て済み IP アドレスのネットマスクを使用します。

（注） 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。

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] を選択します。

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] フィールドで、クライアントに送信されるこのグループ ポリシーに固有の DNS サーバの名前を入力します。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。DNS エントリが複数ある場合は、カンマ、スペース、またはセミコロンで区切ります。

ステップ 5　[Send All DNS Lookups Through Tunnel] フィールドは、VPN トンネル（SSL または IPsec/IKEv2）経由のすべての DNS アドレスを解決するように AnyConnect クライアントに指示します。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 Client は、パブリック DNS サーバ経由でアドレスを解決しようとはしません。[No]（デフォルト）を選択すると、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 クエリーを送信します。

ステップ 6　[Policy] フィールドと [IPv6 Policy] フィールドを設定します。[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、スプリット トンネリング ポリシーを選択して、スプリット トンネリングを設定します。[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 グループ ポリシーである「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 ポリシー設定は [Tunnel All Networks] することです。

[Inherit] チェックボックスをオフにしたら、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]：このポリシーは、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。このオプションは、Cisco VPN Client に対してだけ適用されます。
- [Tunnel Network List Below]：このポリシーでは、[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。このオプションによって、スプリット トンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。それ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。
- [Tunnel All Networks]：このポリシーは、トラフィックを暗号化しないで送信しないこと、または ASA 以外の宛先に送信しないことを指定します。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。

（注）　[Tunnel All Networks] が設定されている場合、AnyConnect では、ローカル DHCP トラフィックはクリア テキストで流れることができます。このために、VPN クライアントが接続すると、特定のルートがローカル DHCP サーバに追加されます。また、このルートでのデータ漏えいを防ぐため、AnyConnect はホスト マシンの LAN アダプタに暗黙的なフィルタを適用し、DHCP トラフィックを除く、そのルートのすべてのトラフィックをブロックします。

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ユニファイド アクセス コントロール リストを選択します。[Inherit] チェックボックスをオフにしないと、グループ ポリシーでは、デフォルト グループ ポリシーで指定されたネットワーク リストが使用されます。デフォルト グループ ポリシーのネットワーク リストのデフォルト値は [None] です。

[Manage] コマンド ボタンを使用して [ACL Manager] ダイアログボックスを開きます。このボックスで、アクセス コントロール リストを設定したり、既存のアクセス コントロール リストを選択してネットワーク リストとして使用したりできます。ネットワーク リストを作成または編集する場合の詳細については、『*Cisco ASA 5500 Series Configuration Guide using ASDM, 6.4 and 6.6*』の第 24 章「Using the ACL Manager」の「Adding ACLs and ACEs」を参照してください。

（注）　拡張 ACL リストは IPv4 アドレスおよび IPv6 アドレスの両方に使用できます。

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。Windows クライアントが XP 以前である場合は、DHCP 代行受信により、ドメイン名およびサブネット マスクが提供されます。

- [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。

ステップ 10　グループ ポリシーにこの変更を行った後、このグループ ポリシーが AnyConnect で使用される接続プロファイルと関連付けられていることを確認します。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択し、接続プロファイルを設定します。

AnyConnect の DNS サーバおよび WINS サーバの設定

DNS サーバおよび WINS サーバは、ネットワーク（クライアント）アクセス グループ ポリシーで設定されています。

内部グループ ポリシーの DNS サーバの設定

内部ネットワーク（クライアント）アクセス グループ ポリシーの DNS サーバを設定するには、次の手順を使用します。

（注）　この設定は、ASDM 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 1　ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Servers] を選択します。

ステップ 2　DefaultGroupPolicy を編集していない限り、[DNS Servers] の [Inherit] チェックボックスをオフにします。

ステップ 3　[DNS Servers] フィールドで、このグループを使用する DNS サーバの IPv4 アドレスまたは IPv6 アドレスを追加します。

DNS サーバ アドレスは最大 4 つ、IPv4 アドレスと IPv6 アドレスで 2 つずつ指定できます。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、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。

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　デフォルト ドメインが [Configuration] > [Remote Access VPN] > [DNS] ウィンドウに指定されていない場合、[Default Domain] フィールドにデフォルト ドメインを指定する必要があります。たとえば、**example.com.** というドメイン名およびトップ レベル ドメインを使用します。

ステップ 6　[OK] をクリックします。

ステップ 7　[Apply] をクリックします。

ステップ 8　グループ ポリシーにこの変更を行った後、このグループ ポリシーが AnyConnect で使用される接続プロファイルと関連付けられていることを確認します。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択し、接続プロファイルを設定します。

内部グループ ポリシーの WINS サーバの設定

プライマリ WINS サーバとセカンダリ WINS サーバを設定するには、次の手順を使用します。それぞれのデフォルト値は none です。

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

ステップ 2　[WINS Servers] の [Inherit] チェックボックスをオフにします。

ステップ 3　[WINS Servers] フィールドに、プライマリ WINS サーバとセカンダリ 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　[OK] をクリックします。

ステップ 5　[Apply] をクリックします。

ステップ 6　グループ ポリシーにこの変更を行った後、このグループ ポリシーが AnyConnect で使用される接続プロファイルと関連付けられていることを確認します。ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択し、接続プロファイルを設定します。

スプリット DNS の機能拡張

AnyConnect 3.1 は、レガシー IPsec クライアントと同様に、Windows プラットフォームと Mac OS X プラットフォーム向けのトゥルー スプリット DNS 機能をサポートしています。セキュリティ アプライアンスのグループ ポリシーにより Split-Include トンネリングが有効になっており、トンネリング対象の DNS 名が指定されている場合、AnyConnect は、この名前に一致するすべての DNS クエリーをプライベート DNS サーバにトンネリングします。トゥルー スプリット DNS を使用すると、ASA によってプッシュダウンされたドメインに一致する DNS 要求へのトンネル アクセスのみが許可されます。こ

れらの要求は、クリア テキストでは送信されません。一方、DNS 要求が ASA によってプッシュダウンされたドメインに一致しない場合は、AnyConnect は、クライアントのオペレーティング システムにある DNS リゾルバから、DNS 解決に使用されるホスト名を暗号化せずに送信させます。

（注） スプリット DNS は、標準クエリーおよび更新クエリー（A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR、CNAME など）をサポートしています。トンネリングされたネットワークのいずれかに一致する PTR クエリーは、トンネル経由で許可されます。

グループ ポリシーによりトンネリングされるドメインが指定されていない場合、または [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [Split Tunneling] で [Tunnel All Networks] が選択されている場合は、AnyConnect はすべての DNS クエリーをトンネリングします。ドメイン名解決には、オペレーティング システムの DNS リゾルバに依存するあらゆるツールまたはアプリケーションを使用できます。たとえば、ping または Web ブラウザを使用してスプリット DNS ソリューションをテストできます。nslookup または dig などのその他のツールは、OS DNS リゾルバを回避します。

この機能には、次のことが必要です。

- 少なくとも 1 台の DNS サーバを設定する
- Split-Include トンネリングの有効にする
- トンネリングするドメインを 1 つ以上指定する
- [Send All DNS lookups through tunnel] チェックボックスをオフにする。このチェックボックスは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [Split Tunneling] にあります。

Mac OS X の場合、AnyConnect は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのトゥルー スプリット DNS を使用できます。

- グループ ポリシーで、スプリット DNS が 1 つの IP プロトコル（IPv4 など）に設定されており、クライアント バイパス プロトコルがもう片方の IP プロトコル（IPv6 など）に設定されている（後者の IP プロトコルにはアドレス プールは設定されていない）。
- スプリット DNS が両方の IP プロトコルに設定されている。

AnyConnect ログによる確認

スプリット DNS が有効化どうか確認するには、AnyConnect のログで、「Received VPN Session Configuration Settings」が含まれたエントリを検索します。有効な場合、このエントリに *Split DNS:enabled* と示されます。IPv4 および IPv6 のスプリット DNS には別々のログ エントリがあります。

スプリット DNS を使用しているドメインの確認

クライアントを使用して、どのドメインがスプリット DNS に使用されているかを確認する手順は次のとおりです。

ステップ 1　**ipconfig/all** を実行して、DNS サフィックス検索リストの横にリストされたドメインを記録します。

ステップ 2　VPN 接続を確立し、DNS サフィックス検索リストの横にリストされたドメインを再度確認します。

トンネルを確立した後に追加されたドメインは、スプリット DNS で使用されるドメインです。

（注）　このプロセスは、ASA からプッシュされたドメインと、クライアント ホストで設定済みのドメインがオーバーラップしていないことを前提としています。

スプリット DNS の設定

この機能を設定するには、セキュリティ アプライアンスへの ASDM 接続を確立して、次の手順を両方とも実行します。

Split-Include トンネリングの設定

ステップ 1　[Configuration] > [Remote AccessVPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [Split Tunneling] を選択します。

ステップ 2　[Policy] ドロップダウン メニューで [Tunnel List Below] を選択し、[Network List] ドロップダウン メニューから該当するネットワーク リストを選択します。

DNS サーバの設定

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

ステップ 2　[DNS Servers] フィールドに、プライベート DNS サーバを 1 つ以上入力します。

ネットワーク ローミング

AnyConnect 3.1 は、IPv4 ネットワークと IPv6 ネットワーク間のローミングに対応しています。AnyConnect が 2 種類のネットワーク間を移動している場合、AnyConnect クライアントは ASA の完全修飾ドメイン名（FQDN）を使用して、そのセキュア ゲートウェイへの接続を維持します。

NAT46 対応ネットワークおよび NAT64 対応ネットワーク（通常は DNS46 設定および DNS64 設定も必要）間のローミングを容易に行うには、クライアントは VPN セッション中にネットワーク ローミングが検出されると必ず ASA FQDN の名前解決を行います。これは、VPN セッションの再確立に使用する ASA IP アドレスを判断するためです。

ロード バランシングを使用している ASA 環境では、ASA の FQDN を設定せずに、ローミング中にプロファイル FQDN を解決できない理由を判断できそうもありません。これは、クライアントが最初に到達する ASA の IP アドレスが、クライアント接続先のデバイスの ASA に属していることを保証できないためです。

（注）　上記の ASA FQDN は、本来、トンネル確立に使用するプロファイル FQDN ではなく、トンネル確立中にクライアントにプッシュされた ASA デバイスの FQDN です。

前提条件

IPv4 ネットワークと IPv6 ネットワーク間のネットワーク ローミングの設定は、ASA のグループ ポリシーで行われます。

内部グループ ポリシーの追加方法または編集方法については、『*ASA Series ASDM Configuration Guide*』の第 73 章「General VPN Setup」の「Configuring Network (Client) Access Internal Group Policies」を参照してください。

IPv4 ネットワークと IPv6 ネットワーク間のネットワーク ローミングの設定

ステップ 1　ASDM を起動し、[Remote Access VPN] > [Configuration] > [Network (Client) Access] > [Group Policies] > [Group Policies] を選択します。

ステップ 2　設定しようとしているグループ ポリシーを選択し、[Edit] をクリックします。

ステップ 3　[Edit Internal Group Policy] ページで [Advanced] > [AnyConnect] をクリックします。

ステップ 4　[FQDN] 行で、[FQDN] チェックボックスをオフにし、[FQDN] テキスト ボックスに ASA の FQDN を追加します。

上記を設定していない場合、ASA は ASA の [Hostname] フィールドおよび [Domain Name] フィールドで定義された FQDN を [Configuration] > [Device Setup] > [Device Name/Password] でプッシュします。ドメイン名は FQDN になるように記入する必要があります。

ドメイン名が FQDN として送信されていない場合、クライアントは ASA の名前解決のみ実行します。それ以外の場合は、AnyConnect は、トンネルを開始して VPN セッションを再確立したときに決定された IP アドレスを使用します。

ステップ 5　変更をグループ ポリシーまたは [Device Name/Password Device Setup] に保存します。

SCEP による認証登録の設定

SCEP を使用した証明書登録に関する情報

セキュア モビリティ スタンドアロン クライアントでは、Simple Certificate Enrollment Protocol（SCEP）を使用して、クライアント認証の一環として証明書のプロビジョニングおよび更新を行うことができます。SCEP の目的は、使用可能な既存のテクノロジーを使用して、スケーラブルな方法で、ネットワーク デバイスに証明書を安全に発行できるようにすることです。

当社の SCEP の実装では、クライアントが証明書要求を開始し、認証局（CA）が自動的に要求を承諾または拒否します。SCEP では、クライアントが証明書を要求してから、承諾または拒否の応答を受信するまで CA にポーリングするという方式も許可されています。ポーリング方式は、このリリースでは実装されていません。

サポートされている登録方式

ASA では、次の 3 つの方式で SCEP を使用した証明書登録がサポートされています。

レガシー SCEP

- クライアントは（VPN トンネルを構築する）ASA に接続し、拡張トンネル経由で CA から証明書を取得します。

- 証明書の期限が切れると、クライアントはこのプロセスを繰り返します。
- これは、AnyConnect 2.4 以降でサポートされています。

SCEP プロキシ

- ASA は SCEP 要求および応答のプロキシとして動作します。クライアントは ASA に接続し、SCEP 要求を送信します。ASA は登録要求を CA に転送し、CA の応答を転送します。クライアントは CA URL に接続する必要はありません。
- VPN プロファイルで証明書失効しきい値が設定されている場合は、ユーザが介入しなくても、クライアントは証明書の期限が切れる前に証明書を更新できます。
- これは、AnyConnect 3.0 以降でサポートされています。

手動 SCEP

- ASA に接続した後、ユーザは SCEP 登録用に設定されたグループを選択します。クライアントには、[Get Certificate] ボタンが表示されたダイアログが表示され、要求は直接 CA に送信されます。この方式では、CA により証明書要求の内容がチェックされないため、他の方式よりも安全性が劣ります。
- 証明書の期限が切れると、クライアントはこのプロセスを繰り返します。

SCEP の登録処理

次に、どのように SCEP 証明書要求が作成され、証明書接続が確立されるかを説明します。

1. クライアントは、証明書ベースの接続プロファイルおよびグループ ポリシー（tunnel-group）を使用して、ASA への接続を試行します。クライアントに有効な証明書が存在しない場合、SCEP がトリガーされます。
2. ASA への接続は、レガシーの場合は AAA、プロキシの場合は AAA と証明書を使用して確立されます。

   手動 SCEP では、フル認証は必要とされません。

   レガシー SCEP および手動 SCEP の場合、この接続では内部 CA へのアクセスが許可されている必要があります。
3. レガシー SCEP の場合、VPN クライアント プロファイルで自動 SCEP ホストが設定されていれば、クライアントは自動的に SCEP 要求を ASA に送信します。

   SCEP プロキシは自動 SCEP ホストを無視し、常に SCEP 要求を送信します。

   手動 SCEP の場合は、ユーザが [Get Certificate] ボタンをクリックしてクレデンシャルを入力すると、SCEP 要求が直接 CA に送信されます。

   証明書要求にマシン ID が使用される場合、クライアントは hostscan をロードしているはずです。
4. SCEP プロキシの場合、ASA は SCEP 要求と CA からの応答をリレーします。

   レガシー SCEP の場合、ASA は CA に要求を転送します。

   手動 SCEP の場合、CA はクライアントに直接応答します。
5. 登録が成功すると、クライアントにユーザに対する（設定可能な）メッセージが表示され、セッションが接続解除されます。クライアントは、証明書および証明書接続プロファイルを使用して、新しいセッションを開始します。

   登録が失敗すると、クライアントに（設定可能な）メッセージが表示され、接続解除されます。

SCEP プロキシの場合、ASA はクライアントから受信した要求をログに記録しますが、接続が失敗した理由は示されません。接続の問題は、CA またはクライアントでデバッグされる必要があります。

一部の CA は、登録パスワードを電子メールでユーザに送信するように設定できます。これにより、セキュリティがより一層強化されます。このパスワードも、AnyConnect クライアント プロファイルで設定できます。これは、CA が証明書を付与する前に確認する、SCEP 要求の一部になります。

自動による証明書要求

AnyConnect レガシー SCEP および SCEP プロキシは、既存のクライアント プロファイルが SCEP ホスト用に設定されていない場合でも、自動証明書要求をサポートします。

- クライアントが設定されている場合：クライアント プロファイルで、証明書登録が有効になっています。クライアントは SCEP を有効にした接続プロファイルでグループ ポリシーを選択し、ASA はクライアントとの VPN 接続を確立して、CA への SCEP 証明書要求を開始します。
- クライアントが設定されていない場合：ユーザが SCEP を有効にした接続プロファイルのグループ URL を選択する必要があります。VPN 接続が確立され、クライアント プロファイルがダウンロードされて、ASA は CA への SCEP 証明書要求を開始します。レガシー SCEP の場合、新しいクライアント プロファイルの自動 SCEP ホストおよび CA の URL が設定されている必要があります。

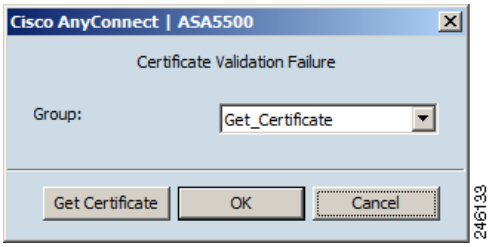
クライアントが自動的に新しい証明書の取得を試行する前に、クライアントの証明書認証は失敗します。

手動証明書要求

ユーザは、クライアント インターフェイスの [Get Certificate] ボタンをクリックすることで、新しい証明書の要求を開始します。手動登録では、ユーザ認証は必要ありません。

手動 SCEP 登録を使用する場合、クライアント プロファイルで CA パスワードを有効にして、証明書登録のセキュリティを強化することをお勧めします。

図 3-10　[Get Certificate] ボタン



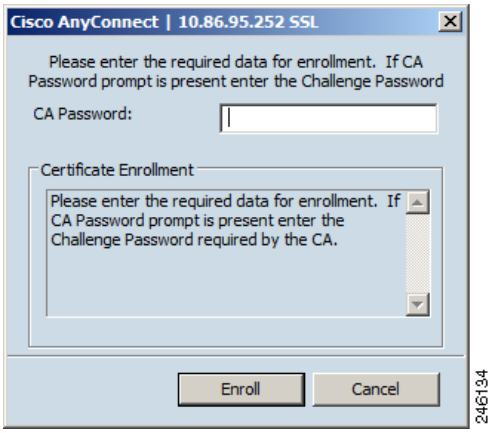
このボタンは、クライアント プロファイルで SCEP 機能が有効になっており、次の条件が満たされている場合にクライアントに表示されます。

- ASA はクライアントから証明書を要求したが、使用可能なホストに受け入れ可能な証明書が存在しない。
- AnyConnect で使用されている現在の証明書が、クライアント プロファイルの [Certificate Expiration Threshold] の設定で定義された日数以内に失効する。AnyConnect で使用されている現在の証明書がすでに失効している。

CA パスワード

クライアント プロファイルで **Prompt For Challenge PW** 属性が有効になっている場合は、ユーザに「CA パスワード」の入力を求めるプロンプトが表示されます。CA パスワードは、ユーザを識別するための認証局に送信されるチャレンジ パスワードまたはトークンです。次に、[Enroll] ボタンが表示された [CA Password] ウィンドウの図を示します。

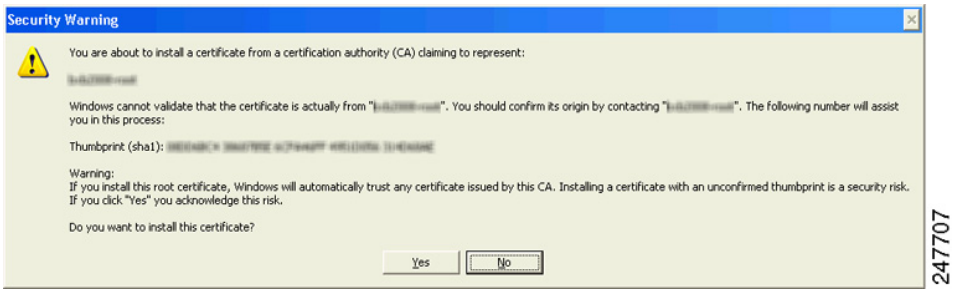
図 3-11　[CA Password] ウィンドウ



Windows 証明書の警告

Windows クライアントが初めて認証局から証明書を取得しようとした場合、それが自動か手動かによらず図 3-12 のような警告が表示されることがあります。プロンプトが表示されたら、[Yes] をクリックしてください。これにより、ルート証明書をインポートできるようになります。クライアント証明書を使用して接続する機能には影響ありません。

図 3-12　Windows 証明書のセキュリティ警告



SCEP を使用した証明書登録のガイドラインと制限

- SCEP 要求は、クライアント プロファイルにより開始されます。SCEP は、その他の証明書認証よりも優先されます。

- SCEP は、AnyConnect をサポートしているすべてのオペレーティング システムでサポートされています。
- ロードバランシングがサポートされています。
- クライアントレス（ブラウザベース）でのアクセスは SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）ではサポートしています。
- 証明書要求にマシン ID が使用される場合、クライアントは hostscan をロードしている必要があります。

SCEP を使用した証明書登録の前提条件

- AnyConnect セキュア モビリティ クライアント 3.0 以降がエンドポイントで実行中である必要があります。
- CA は自動付与モードである必要があります。証明書のポーリングはサポートされません。
- レガシー SCEP および手動 SCEP の場合、プライベート CA は ASA にアクセス可能である必要があります。
- ASA は AnyConnect SSL または IKEv2 VPN セッションを使用する必要があります。
- IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含め、すべての SCEP 準拠 CA がサポートされています。

SCEP による認証登録の設定

SCEP 登録用 VPN クライアント プロファイルの設定

ステップ 1　ASDM からプロファイル エディタを起動するか、またはスタンドアロンの VPN プロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　ASDM では、[Add]（または [Edit]）をクリックして、AnyConnect プロファイルを作成（または編集）します。スタンドアロン エディタでは、既存のプロファイルを開くか、新しいプロファイルの作成を続行します。

ステップ 3　左側の [AnyConnect Client Profile] ツリーで、[Certificate Enrollment] をクリックします。

ステップ 4　[Certificate Enrollment] ペインで、[Certificate Enrollment] をオンにします。

ステップ 5　レガシー SCEP のみ、証明書を取得するためにクライアントをリダイレクトする [Automatic SCEP Host] を指定します。FQDN または IP アドレス、および SCEP 証明書取得用に設定された接続プロファイル（トンネル グループ）を入力します。たとえば、ASA の名前として **asa.cisco.com**、接続プロファイルの名前として **scep_eng** を入力します。

ステップ 6　レガシー SCEP のみ、SCEP CA サーバを識別するための CA URL を指定します。FQDN または IP アドレスを入力します（**http://ca01.cisco.com** など）。

ステップ 7　（任意）ユーザに対して、そのユーザ名および 1 回限定利用のパスワードに関するプロンプトを表示する場合は、[Prompt For Challenge PW] をオンにします。

ステップ 8　（任意）CA 証明書のサムプリントを入力します。SHA1 ハッシュまたは MD5 ハッシュを使用します（`8475B661202E3414D4BB223A464E6AAB8CA123AB` など）。

（注）　CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行された証明書の「fingerprint」または「thumbprint」属性フィールドからではなく、サーバから直接取得します。

ステップ 9　登録証明書で、要求する [Certificate Contents] を設定します。証明書フィールドの定義については、「AnyConnect プロファイル エディタの [Certificate Enrollment]」（P.3-89）を参照してください。

（注）　%machineid% を使用した場合は、クライアントに Hostscan/Posture がロードされます。

ステップ 10　[Display Get Certificate Button] をオンして、認証証明書のプロビジョニングや更新をユーザが手動で行えるようにします。このボタンは、サーバでの証明書照合が失敗した場合に表示されます。

ステップ 11　（任意）[General] ペインで、SCEP 接続プロファイルに [Connection Profile (Tunnel Group) Lock] を設定します。これにより、SCEP が設定された接続プロファイルへのトラフィックが制限されます。

ステップ 12　（任意）サーバ リストで特定のホストに対して SCEP を有効にします。これにより、ステップ 4 の SCEP ホスト設定は上書きされます。[Server List] ペインに移動し、既存のホスト エントリを編集するか、または SCEP ホストを使用して新規のホスト エントリを作成します。サーバ リストの設定の詳細については、<<add link>> を参照してください。

SCEP プロキシをサポートするための ASA の設定

次に、ASA で SCEP プロキシをサポートするように ASA を設定する高度な手順について説明します。SCEP プロキシでは、1 つの接続プロファイルで、証明書接続および証明書登録をサポートします。

ステップ 1　「SCEP 登録用 VPN クライアント プロファイルの設定」（P.3-49）のプロファイルの作成手順に従って、クライアント プロファイル（例：ac_scep）を作成します。

ステップ 2　グループ ポリシー（例：certgroup）を作成します。

- [General] で、[SCEP Forwarding URL] に CA への URL を入力します。
- [Advanced] > [AnyConnect Client] で、[Inherit for Client Profiles to Download] をオフにし、SCEP のクライアント（ac_scep）を追加します。

ステップ 3　登録用の接続プロファイル（例：certtunnel）を作成します。

- [Authentication]：Both（AAA および Certificate）
- [Default Group Policy]：certgroup
- [Advanced] > [General] で、[Enable SCEP Enrollment for this tunnel] をオンにします。
- [Advanced] > [SSL VPN Client] の [Client Profile to Download] で、ac_scep クライアント プロファイルを選択します。
- [Advanced] > [GroupAlias/Group URL] で、この接続プロファイルのグループ（centgroup）が含まれるグループ URL を作成します。

SCEP レガシーをサポートするための ASA の設定

ステップ 1　「SCEP 登録用 VPN クライアント プロファイルの設定」（P.3-49）のプロファイルの作成手順に従って、クライアント プロファイル（例：ac_scep）を作成します。このプロファイルに CA URL が設定されていることを確認します。

ステップ 2　登録用のグループ ポリシー（例：certenroll）を作成します。

ステップ 3　認証用の 2 つ目のグループ ポリシー（例：certauth）を作成します。

ステップ 4　登録用の接続プロファイル（例：scep_cp）を作成します。

- [Authentication]：AAA
- [Default Group Policy]：certenroll
- [Advanced] > [SSL VPN Client] の [Client Profile to Download] で、ac_sep クライアント プロファイルを選択します。
- [Advanced] > [GroupAlias/Group URL] で、この接続プロファイルの登録グループ（centroll）が含まれるグループ URL を作成します。

  ASA ではこの接続プロファイルを有効にしないでください。ユーザにグループを公開しなくても、ユーザはグループにアクセスできます。

ステップ 5　認証用の接続プロファイル（例：centauth）を作成します。

- [Authorization]：Certificate

  ASA ではこの接続プロファイルを有効にしないでください。ユーザにグループを公開しなくても、ユーザはグループにアクセスできます。

ASA における証明書のみの認証の設定

複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルと共に、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、ASA に開発部の Department_OU 値をプロビジョニングし、このプロセスによる証明書が ASA に提供された時点でこのグループにユーザが配置されるようにすることができます。

SCEP の DAP レコード

aaa.cisco.sceprequired：この属性を使用して登録接続を確立し、適切な制限ポリシーを選択したレコードに適用できます。

証明書の失効通知の設定

ユーザに対して証明書の失効が近いことを警告できるように、クライアント プロファイルを設定することができます。[Certificate Expiration Threshold] の設定では、AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するかを指定します。

（注）　RADIUS 登録では、[Certificate Expiration Threshold] 機能は使用できません。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Add]（または [Edit]）をクリックして AnyConnect プロファイルを作成（または編集）し、左側の [AnyConnect Client Profile] ツリーで [Certificate Enrollment] をクリックします。

ステップ 3　[Certificate Enrollment] ペインで、[Certificate Enrollment] をオンにします。

ステップ 4　AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するかを表す証明書失効しきい値を指定します。

デフォルトは 0（警告は表示しない）です。範囲は 0 ～ 180 日です。

ステップ 5　[OK] をクリックします。

証明書ストアの設定

AnyConnect がクライアントのシステムの証明書ストアを見つけ、処理する方法を設定できます。プラットフォームによっては、特定ストアへのアクセスが制限される場合や、ブラウザ ベースのストアの代わりにファイルを使用できる場合があります。この目的は、クライアント証明書の使用だけでなく、サーバ証明書の確認のための適切な場所に AnyConnect を振り向けることです。

Windows では、クライアントがどの証明書ストアで証明書を検索するかを制御できます。証明書の検索をユーザ ストアのみ、またはマシン ストアのみに制限するようにクライアントを設定できます。Mac および Linux では、PEM 形式の証明書ファイル用の証明書ストアを作成できます。

これらの証明書ストアの検索設定は、AnyConnect クライアント プロファイルに格納されます。

（注）　また、AnyConnect ローカル ポリシーに、さらに証明書ストアの制約を設定できます。AnyConnect ローカル ポリシーは、企業のソフトウェア展開システムを使用して展開する XML ファイルであり、AnyConnect クライアント ファイルからは独立しています。ファイル内の設定により、Firefox NSS（Linux と Mac）、PEM ファイル、Mac ネイティブ（キーチェーン）、および Windows Internet Explorer ネイティブ証明書ストアの使用が制限されます。詳細については、第 8 章「FIPS と追加セキュリティの有効化」を参照してください。

ここでは、証明書ストアを設定し、その使用を制御する手順について説明します。

- 「Windows での証明書ストアの制御」（P.3-52）
- 「Mac および Linux での PEM 証明書ストアの作成」（P.3-54）

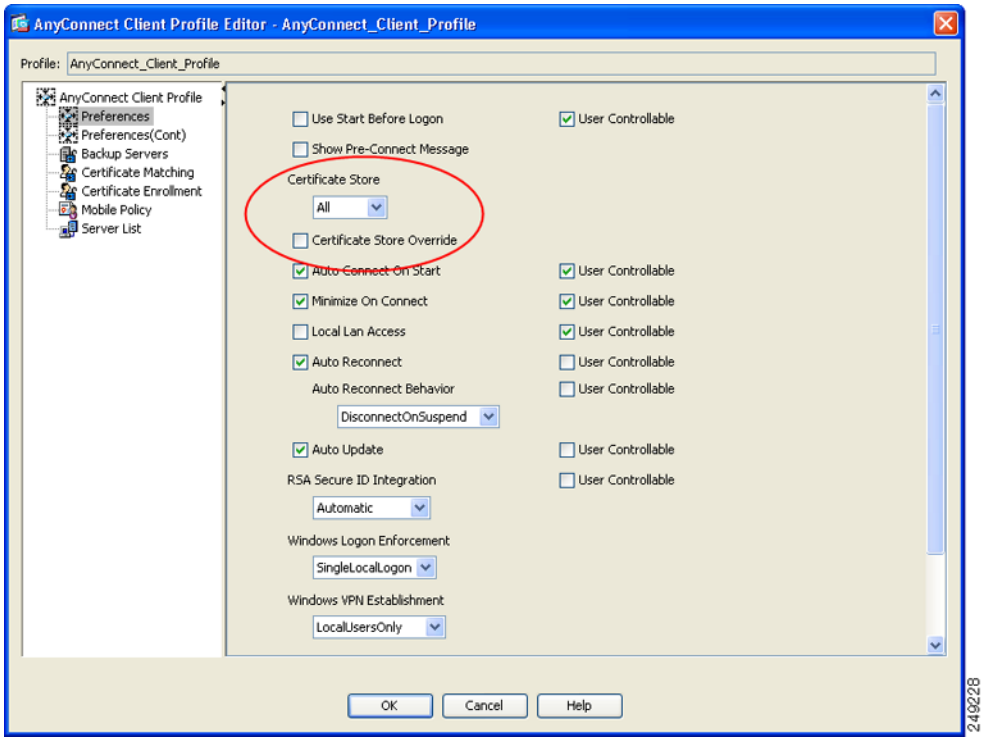
Windows での証明書ストアの制御

Windows では、ローカル マシン用の証明書ストアと現在のユーザ用の証明書ストアが別々に用意されます。クライアント プロファイルは、AnyConnect クライアントがどの証明書ストアで証明書を検索するかを指定します。

コンピュータ上で管理者権限を持つユーザは、両方の証明書ストアにアクセスできます。管理者権限を持たないユーザがアクセスできるのは、ユーザ証明書ストアのみです。通常、Windows XP ユーザには、管理者権限がありますが、Windows 7 ユーザにはありません。

AnyConnect がどの証明書ストアで証明書を検索するかは、プロファイル エディタの [Preferences (Part 1)] ペインにある [Certificate Store] リスト ボックスを使用して設定します。[Certificate Store Override] チェックボックスを使用すると、AnyConnect では非管理者権限を持つユーザでもマシン証明書ストアを検索できるようになります。

図 3-13　[Certificate Store] リスト ボックスと [Certificate Store Override] チェックボックス



[Certificate Store] は次の 3 つの設定が可能です。

- [All]：（デフォルト）すべての証明書ストアを検索します。
- [Machine]：マシン証明書ストア（コンピュータで識別された証明書）を検索します。
- [User]：ユーザ証明書ストアを検索します。

[Certificate Store Override] は次の 2 つの設定が可能です。

- オン：ユーザが管理者権限を持っていない場合でも、AnyConnect は、コンピュータのマシン証明書ストアを検索できます。
- オフ：（デフォルト）AnyConnect は、管理者権限のないユーザのマシン証明書ストアを検索できません。

表 3-4 は、[Certificate Store] および [Certificate Store Override] の設定例を示したものです。

表 3-4　証明書ストアと証明書ストア上書き設定の例

[Certificate Store] の設定	[Certificate Store Override] の設定	AnyConnect の処理
All	オフ	AnyConnect は、すべての証明書ストアを検索します。ユーザが非管理者権限を持っている場合、AnyConnect は、マシン ストアにアクセスできません。 これはデフォルトの設定です。ほとんどの場合、この設定が適しています。変更が必要となる特別な理由またはシナリオ要件がある場合を除いて、この設定は変更しないでください。
All	オン	AnyConnect は、すべての証明書ストアを検索します。ユーザが管理者以外の権限を持っている場合、AnyConnect は、マシン ストアにアクセスできます。
Machine	オン	AnyConnect は、マシン証明書ストアを検索します。AnyConnect は、非管理者アカウントのマシン ストアを検索することができます。
Machine	オフ	AnyConnect は、マシン証明書ストアを検索します。ユーザが管理者以外の権限を持っている場合、AnyConnect は、マシン ストアを検索できません。 **（注）** 証明書を使用する認証が限定されたユーザのグループにのみ許可されている場合、この設定が使用される場合があります。
User	適用されない	AnyConnect は、ユーザ証明書ストア内のみ検索します。非管理者アカウントがこの証明書ストアにアクセス権を持つため、証明書ストアの上書きは適用されません。

Mac および Linux での PEM 証明書ストアの作成

AnyConnect は、Privacy Enhanced Mail（PEM）形式のファイル ストアを使用した証明書認証をサポートしています。ブラウザに依存して証明書の確認および署名を行う代わりに、クライアントがリモート コンピュータのファイル システムから PEM 形式の証明書ファイルを読み取り、確認と署名を行います。

PEM ファイルのファイル名に関する制約事項

あらゆる条件下でクライアントが適切な証明書を取得するためには、ファイルが次の要件を満たしている必要があります。

- すべての証明書ファイルは、拡張子 **.pem** で終わっていること。
- すべての秘密キー ファイルは、拡張子 **.key** で終わっていること。
- クライアント証明書と、それに対応する秘密キーのファイル名が同じであること（client.pem と client.key など）。

（注）　PEM ファイルのコピーを保持する代わりに、PEM ファイルへのソフト リンクを使用できます。

ユーザ証明書の保存

PEM ファイル証明書ストアを作成する場合は、表 5 に示すパスとフォルダを作成します。これらのフォルダに、適切な証明書を配置してください。

表 5　PEM ファイル証明書ストアのフォルダと保存される証明書のタイプ

PEM ファイル証明書ストアのフォルダ	保存される証明書のタイプ
~/.cisco/certificates/ca[1]	信頼できる CA とルート証明書
~/.cisco/certificates/client	クライアント証明書
~/.cisco/certificates/client/private	秘密キー

1. ~ は、ホーム ディレクトリを表します。

（注）　マシン証明書の要件は、PEM ファイル証明書の要件と同じですが、ルート ディレクトリが異なります。マシン証明書の場合は、~/.cisco を /opt/.cisco に置き換えてください。それ以外は、表 5 に示すパス、フォルダ、および証明書のタイプが適用されます。

証明書照合の設定

AnyConnect は、次の証明書照合タイプをサポートしています。これらの一部またはすべてを使用して、クライアント証明書を照合できます。証明書照合は、[Certificate Matching] ペインの AnyConnect VPN クライアント プロファイルで設定できるグローバル基準です。基準は次のとおりです。

- キーの用途
- キーの拡張用途
- 識別名

プロファイルには、0 個以上の一致基準を含めることができます。証明書が一致すると見なされるには、指定されているすべての基準に一致している必要があります。

証明書キーの用途による照合

証明書照合キーの用途は、ある特定の証明書で実行可能な幅広い操作に対する制約のセットとして与えられます。サポート対象のセットは、VPN クライアント プロファイルの *Key Usage* リストに一覧表示されており、次が含まれています。

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN

- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

プロファイルには、0 個以上の一致基準を含めることができます。1 つ以上の基準が指定されている場合、証明書が一致すると見なされるには、少なくとも 1 つの基準が一致している必要があります。

「証明書照合の例」（P.3-58）の例には、これらの属性を設定する方法が記載されています。

証明書キーの拡張用途による照合

この照合により管理者は、VPN クライアント プロファイルの [Extended Key Usage] フィールドに基づいて、クライアントが使用できる証明書を制限できます。表 3-6 は、既知の制約のセットと、それに対応するオブジェクト ID（OID）をリストにまとめたものです。

表 3-6　証明書キーの拡張用途

制約	OID
ServerAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE Intermediate	1.3.6.1.5.5.8.2.2

カスタム拡張照合キー

その他の OID（本書の例で使用している 1.3.6.1.5.5.7.3.11 など）はすべて、「カスタム」と見なされます。管理者は、既知のセットの中に必要な OID がない場合、独自の OID を追加できます。

証明書の識別名による照合

クライアント プロファイルの [Certificate Matching] ペインの [Distinguished Name] テーブルには、クライアントで使用できる証明書を指定された基準および基準照合条件に一致する証明書に制限する証明書 ID が入っています。[Add] ボタンをクリックすると、いずれかの基準をリストに追加し、値またはワイルドカードを設定してその基準の内容と照合させることができます。表 3-7 にサポート対象の基準を一覧表示します。

表 3-7　証明書の識別名による照合の基準

ID	説明
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

プロファイルには、0 個以上の一致基準を含めることができます。証明書が一致すると見なされるには、指定されているすべての基準に一致している必要があります。*識別名*による照合によって、追加の照合基準が提供されます。たとえば、管理者が、指定した文字列が証明書に含まれている必要があるか、含まれていてはいけないかを指定できます。また、文字列のワイルドカードも使用できます。

証明書照合の例

（注）　これ以降の例で使用する KeyUsage、ExtendedKeyUsage、および DistinguishedName のプロファイル値はあくまでも例です。証明書一致基準は、使用する証明書に適用するもののみ設定してください。

クライアント プロファイルで証明書照合を設定する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Certificate Matching] ペインに移動します。

ステップ 3　[Key Usage] および [Extended Key Usage] の設定をオンにし、受け入れ可能なクライアント証明書を選択します。指定されたキーの少なくとも 1 つが一致する証明書が選択されます。これらの用途設定に関する詳細については、「AnyConnect プロファイル エディタの [Certificate Matching]」（P.3-87）を参照してください。

ステップ 4　カスタム拡張照合キーを指定します。これらは、1.3.6.1.5.5.7.3.11 など既知の MIB OID 値であることが必要です。0 個以上のカスタム拡張照合キーを指定することができます。指定されたすべてのキーが一致する証明書が選択されます。キーは、OID 形式であることが必要です （1.3.6.1.5.5.7.3.11 など）。

ステップ 5　[Distinguished Names] テーブルの横にある [Add] をクリックして、[Distinguished Name Entry] ウィンドウを起動します。

- [Name]：識別名。
- [Pattern]：照合に使用する文字列。照合するパターンには、目的の文字列部分のみ含まれている必要があります。パターン照合構文や正規表現構文を入力する必要はありません。入力した場合、その構文は検索対象の文字列の一部と見なされます。

  abc.cisco.com という文字列を例とした場合、cisco.com で照合するためには、入力するパターンを cisco.com とする必要があります。
- [Operator]：照合を実行する際に使用する演算子。
  - [Equal]：== と同等
  - [Not Equal]：!= と同等
- [Wildcard]：ワイルドカード パターン照合を使用します。このパターンは文字列内のどの場所でも使用できます。
- [Match Case]：有効にすると、大文字と小文字を区別したパターン照合を実行できます。

認証証明書選択のプロンプト

ユーザに対して有効な証明書のリストを表示し、セッションに認証に使用する証明書をユーザが選択できるように AnyConnect の設定を行うことができます。この設定は、Windows 7、Windows Vista、および Windows XP でのみ行うことができます。デフォルトの場合、ユーザの証明書選択は無効です。

証明書の選択を有効にするには、AnyConnect プロファイルで次の作業を実行します。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

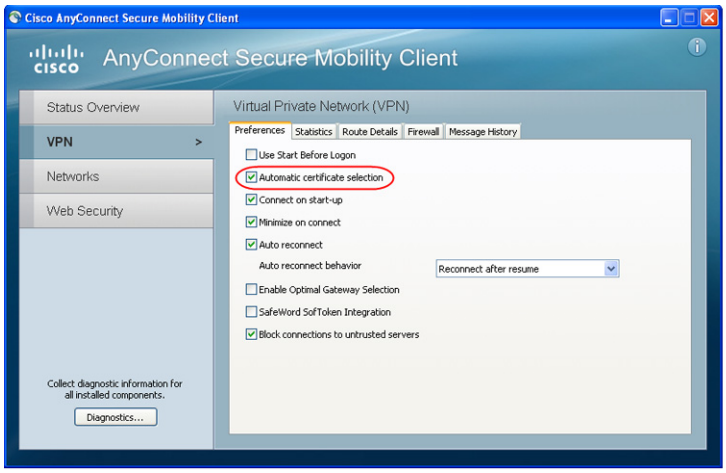
ステップ 2　[Preferences (Part 2)] ペインに移動し、[Disable Certificate Selection] をオフにします。これによりクライアントでは、ユーザに対して認証証明書を選択するためのプロンプトが表示されます。

ユーザによる AnyConnect プリファレンスでの自動証明書選択の設定

ユーザの証明書選択を有効にすると、AnyConnect の [Preferences] ダイアログボックスに、[Automatic Certificate Selection] チェックボックスが表示されます。ユーザは、[Automatic certificate selection] チェックボックスをオンまたはオフにすることで、自動証明書選択をオンまたはオフにできます。

図 3-19 は、[Preferences] ウィンドウに表示された [Automatic Certificate Selection] チェックボックスを示します。

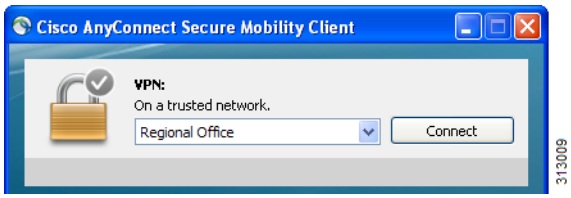
図 3-14　[Automatic Certificate Selection] チェックボックス



サーバ リストの設定

プロファイルの主要な使用目的の 1 つは、ユーザが接続サーバをリストできるようにすることです。このサーバ リストは、ホスト名とホスト アドレスのペアで構成されています。ホスト名は、ホストを参照するために使用するエイリアスのほか、FQDN、または IP アドレスにできます。サーバ リストには、AnyConnect GUI の [*Connect to*] ドロップダウン リスト（図 3-20）にあるサーバのホスト名が一覧表示されます。ユーザはこのリストからサーバを選択できます。

図 3-15　[Connect to] ドロップダウン リストにホストが表示されたユーザ GUI



最初は、リストの先頭にある設定したホストがデフォルト サーバとなり、GUI ドロップダウン リストに表示されます。ユーザがリストから別のサーバを選択すると、クライアントではその選択内容がリモート コンピュータ上のユーザ プリファレンス ファイルに記録され、選択されたサーバが新たなデフォルト サーバとなります。

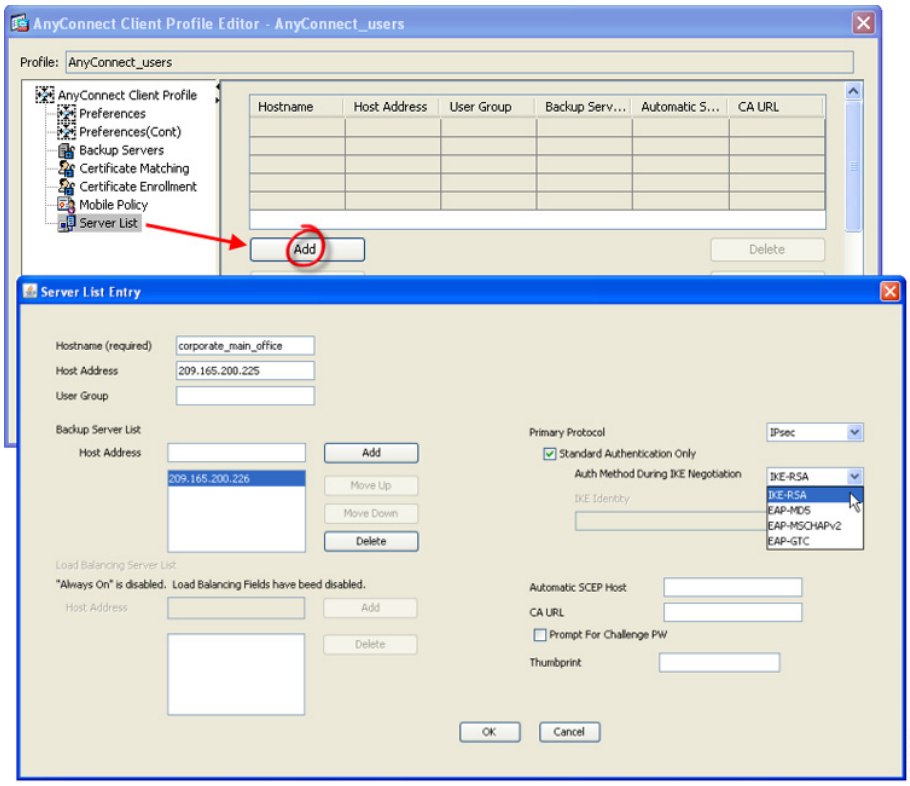
サーバ リストを設定する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Server List] をクリックします。[Server List] ペインが開きます。

ステップ 3　[Add] をクリックします。[Server List Entry] ウィンドウが開きます（図 3-21）。

図 3-16　サーバ リストの追加



ステップ 4　ホスト名を入力します。ホスト名は、ホストを参照するために使用するエイリアスのほか、FQDN、または IP アドレスにできます。

FQDN または IP アドレスを入力した場合、ホスト アドレスを入力する必要はありません。

IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイの使用はサポートしていません。

ステップ 5　必要に応じてホスト アドレスを入力します。

ステップ 6　ユーザ グループを指定します（任意）。クライアントでは、このユーザ グループとホスト アドレスを組み合わせてグループ ベースの URL が構成されます。

（注）　プライマリ プロトコルを IPsec として指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。

ステップ 7　（AnyConnect リリース 3.0.1047 以降の場合）。モバイルデバイス用のサーバ リストを設定するには、[Additional mobile-only settings] チェックボックスをオンにして、[Edit] をクリックします。詳細については、「サーバ リストの設定」のモバイル デバイス用の設定についての説明を参照してください。

ステップ 8　バックアップ サーバを追加します（任意）。サーバ リスト内のサーバが使用できない場合、クライアントではグローバル バックアップ サーバ リストを使用する前に、そのサーバのバックアップ リストにあるサーバへの接続が試行されます。

ステップ 9　ロード バランシング バックアップ サーバを追加します（任意）。このサーバ リスト エントリのホストがセキュリティ アプライアンスのロード バランシング クラスタであり、かつ常時接続機能が有効になっている場合は、このリストでクラスタのバックアップ デバイスを指定します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスは常時接続機能によりブロックされます。

ステップ 10　この ASA に対して使用するクライアントのプライマリ プロトコル（SSL または IKEv2 を使用した IPsec）を指定します（任意）。デフォルトは SSL です。デフォルトの認証方式（独自の AnyConnect EAP 方式）を無効にするには、[Standard Authentication Only] をオンにし、ドロップダウン リストから方式を選択します。

（注）　認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、ASA でセッション タイムアウト、アイドル タイムアウト、接続解除タイムアウト、スプリット トンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

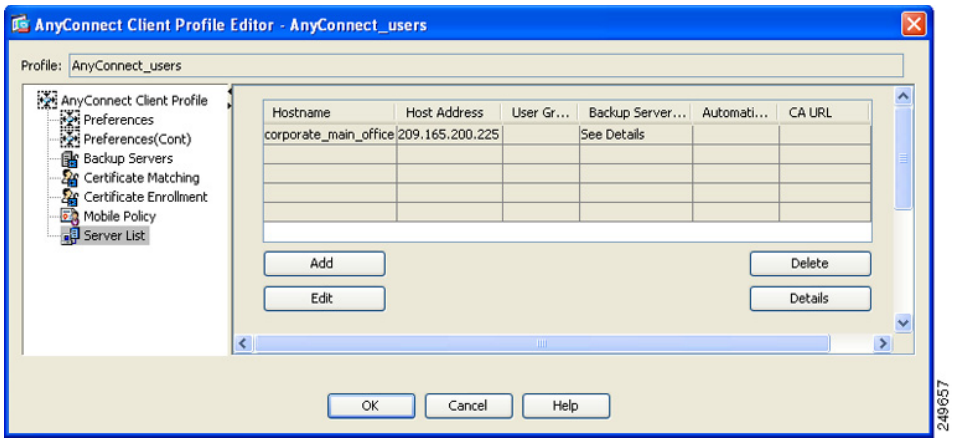
ステップ 11　SCEP CA サーバの URL を指定します（任意）。FQDN または IP アドレスを入力します（http://ca01.cisco.com など）。

ステップ 12　[Prompt For Challenge PW] をオンにして（任意）、ユーザが証明書を手動で要求できるようにします。ユーザが [Get Certificate] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。

ステップ 13　CA の証明書サムプリントを入力します。SHA1 ハッシュまたは MD5 ハッシュを使用します CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行した証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

ステップ 14　[OK] をクリックします。設定した新規のサーバ リスト エントリが、サーバ リスト テーブルに表示されます（図 3-22）。

図 3-17　新規のサーバ リスト エントリ



モバイル デバイス用接続設定

前提条件

- 「サーバ リストの設定」（P.3-60）のステップ 1 ～ 6 を実行します。
- バージョン 3.0.1047 以降のプロファイル エディタを使用する必要があります。
- Apple iOS バージョン 4.1 以降を実行する Apple モバイルデバイスでサポートされます。

ガイドライン

ASA からモバイル デバイスに配信された AnyConnect VPN クライアント プロファイルは、再設定したり、モバイル デバイスから削除したりすることはできません。ユーザが、新しい VPN 接続用にデバイス上で独自のクライアント プロファイルを作成した場合は、そのプロファイルを設定、編集、削除できます。

手順の詳細

ステップ 1　[Server List Entry] ダイアログボックスで、[Additional mobile-only settings] をオンにして [Edit] をクリックします。

ステップ 2　[Apple iOS / Android Settings] エリアでは、Apple iOS または Android オペレーティング システムを実行するデバイスに、次の属性を設定できます。

a. 証明書認証タイプを選択します。

- [Automatic] : AnyConnect では、認証で使用されるクライアント証明書が自動的に選択されます。この場合、インストールされているすべての証明書が確認されて期限切れの証明書が無視され、VPN クライアント プロファイルに定義された基準に一致する証明書が適用されます。次に、基準に一致する証明書を使用して認証されます。これは、ユーザが VPN 接続の確立を試行するたびに実行されます。

- [Manual]：AnyConnect は、自動認証と同様に認証で使用される証明書を検索します。ただし、手動証明書認証タイプでは、VPN クライアント プロファイルで定義された一致条件に一致する証明書がいったん検出されると、AnyConnect はその証明書を接続用に割り当てます。この場合、ユーザが新しい VPN 接続の確立を試行しても、新しい証明書の検索は行われません。
- [Disabled]：認証にクライアント証明書は使用されません。

b. [Make this Server List Entry active when profile is imported] チェックボックスをオンにした場合、VPN プロファイルがデバイスにダウンロードされたときに、このサーバ リスト エントリをデフォルトの接続として定義したことになります。この宛先を設定できるのは、1 つのサーバ リスト エントリのみです。デフォルトではオフになっています。

ステップ 3　[Apple iOS Only Settings] エリアでは、Apple iOS を実行するデバイスのみに、次の属性を設定できます。

a. [Reconnect when roaming between 3G/Wifi networks] チェックボックスを設定します。デフォルトではこのボックスはオンになっており、3G ネットワークと Wifi ネットワークの切り替え時に、AnyConnect は VPN 接続を維持するように試行します。このボックスをオフにすると、3G ネットワークと Wifi ネットワークの切り替え時に、AnyConnect は VPN 接続を維持するように試行しません。

b. [Connect on Demand] チェックボックスを設定します。

このエリアを使用して、Apple iOS から提供される Connect on Demand 機能を設定できます。その他のアプリケーションが、ドメイン ネーム システム（DNS）を使用して解決されるネットワーク接続を開始したときに、その都度チェックされるルールのリストを作成できます。

[Connect on Demand] は、[Certificate Authentication] フィールドが [Manual] または [Automatic] に設定されている場合のみオンにできます。[Certificate Authentication] フィールドが [Disabled] に設定されている場合は、このチェックボックスはグレー表示されます。[Match Domain or Host] フィールドおよび [On Demand Action] フィールドで定義される Connect on Demand ルールは、チェックボックスがグレー表示されている場合でも、設定および保存できます。

c. [Match Domain or Host] フィールドに、Connect on Demand ルールを作成する対象のホスト名（host.example.com）、ドメイン名（.example.com）、または部分ドメイン（.internal.example.com）を入力します。このフィールドには、IP アドレス（10.125.84.1）を入力しないでください。

d. [On Demand Action] フィールドで、ユーザが前のステップで定義したドメインまたはホストへの接続を試行したときに実行されるアクションを、次のいずれかに指定します。

- [Always connect]：このリストのルールに一致したときに、iOS は必ず VPN 接続の開始を試行します。
- [Connect if needed]：このリストのルールに一致したときに、システムが DNS を使用してアドレスを解決できなかった場合に限り、iOS は VPN 接続の開始を試行します。
- [Never connect]：このリストのルールに一致しても、iOS は絶対に VPN 接続の開始を試行しません。[Always connect] または [Connect if needed] のルールよりも、このリストのルールが優先されます。

  Connect On Demand が有効の場合、アプリケーションは自動的にこのリストにサーバ アドレスを追加します。これにより、Web ブラウザを使用してサーバのクライアントレス ポータルへのアクセスを試行する場合は、VPN 接続が自動的に確立されなくなります。この動作を望まない場合は、このルールを削除できます。

e. [Match Domain or Host] フィールドおよび [On Demand Action] フィールドを使用してルールを作成したら、[Add] をクリックします。

このルールが、下部のルール リストに表示されます。

ステップ 4　[OK] をクリックします。

ステップ 5　「サーバ リストの設定」（P.3-60）のステップ 8 に戻ります。

バックアップ サーバ リストの設定

ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定できます。これらのサーバは、AnyConnect プロファイルの [Backup Servers] ペインで指定します。場合によっては、このリストでホスト固有の設定を指定することがあります。手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Backup Servers] ペインに移動し、バックアップ サーバのホスト アドレスを入力します。

Connect On Start-up の設定

Connect on Start-up は、VPN クライアント プロファイルで指定されたセキュア ゲートウェイを使用して、自動的に VPN 接続を確立します。接続時、クライアントでは、セキュア ゲートウェイから提供されたプロファイルとローカル プロファイルが同じでない場合、セキュア ゲートウェイから提供されたプロファイルでローカル プロファイルが置き換えられ、このプロファイルの設定が適用されます。

デフォルトでは、Connect on Start-up は**無効**です。ユーザが AnyConnect クライアントを起動すると、GUI にはユーザ制御可能設定としてデフォルトの設定が表示されます。ユーザは、GUI の [Connect to] ドロップダウン リストでセキュア ゲートウェイの名前を選択し、[Connect] をクリックする必要があります。接続時、クライアントでは、セキュリティ アプライアンスから提供されたクライアント プロファイルの設定が適用されます。

AnyConnect は、AnyConnect の起動時に自動的に VPN 接続を確立する機能から、ログイン後の VPN 常時接続機能により、その VPN 接続を「常時接続」にする機能に進化しました。Connect on Start-up 要素のデフォルトが無効になっているのは、この進化を反映しているためです。企業の展開で Connect on Start-up 機能を使用している場合は、この代わりに Trusted Network Detection を使用することを検討してください。

Trusted Network Detection（TND）を使用すると、ユーザが企業ネットワークの中（信頼ネットワーク）にいる場合は AnyConnect により自動的に VPN 接続が解除され、企業ネットワークの外（非信頼ネットワーク）にいる場合は自動的に VPN 接続が開始されるようにすることができます。この機能を使用すると、ユーザが信頼ネットワークの外にいるときに VPN 接続を開始することによって、セキュリティ意識を高めることができます。Trusted Network Detection の設定の詳細については、「Trusted Network Detection の設定」（P.3-21）を参照してください。

デフォルトでは、Connect on Start-up は無効です。有効にするには、次の手順に従います。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　ナビゲーション ペインで [Preferences] を選択します。

ステップ 3　[Connect On Start-up] をオンにします。

自動再接続の設定

IPsec VPN クライアントとは異なり、AnyConnect は、初期接続に使用したメディアによらず、VPN セッションの中断から復旧することおよびセッションを再確立することができます。たとえば、有線、ワイヤレス、または 3G のセッションを再確立できます。

自動再接続機能を設定すると、接続が解除された場合に VPN 接続の再確立が試行されます（デフォルトの動作）。また、*システムの一時停止*または*システムのレジューム*が発生して以降に接続の動作を定義することもできます。システムの一時停止とは、低電力スタンバイ、Windows の「休止状態」、Mac OS または Linux の「スリープ」のことです。システムのレジュームとは、システムの一時停止からの回復です。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　ナビゲーション ペインで [Preferences (Part 1)] を選択します。

ステップ 3　[Auto Reconnect] をオンにします。

（注）　[*Auto Reconnect*] をオフにすると、クライアントでは接続解除の原因にかかわらず、再接続が試行されません。

ステップ 4　自動再接続の動作を選択します（Linux ではサポートされていません）。

- [Disconnect On Suspend]：AnyConnect では、システムが一時停止すると VPN セッションに割り当てられたリソースが解放され、システムのレジューム後も再接続は試行されません。
- [Reconnect After Resume]：クライアントでは、システムが一時停止すると VPN セッションに割り当てられたリソースが保持され、システムのレジューム後は再接続が試行されます。

ローカル プロキシ接続

デフォルトでは、ユーザは AnyConnect でローカル PC 上のトランスペアレントまたは非トランスペアレントのプロキシを介して VPN セッションを確立するようになっています。

次に示すのは、透過的なプロキシ サービスを実現する要素の一例です。

- 一部のワイヤレス データ カードから入手できるアクセラレーション ソフトウェア
- Kaspersky など一部のアンチウイルス ソフトウェア上のネットワーク コンポーネント

ローカル プロキシ接続に関する要件

AnyConnect は、次の Microsoft OS 上でこの機能をサポートしています。

- Windows 7（32 ビットおよび 64 ビット）
- Windows Vista（32 ビットおよび 64 ビット）SP2 または KB952876 を適用した Vista Service Pack 1
- Windows XP SP3

この機能をサポートするためには、AnyConnect Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition ライセンスのどちらかが必要です。

ローカル プロキシ接続の設定

AnyConnect は、VPN セッションを確立するためのローカル プロキシ サービスをデフォルトでサポートしています。AnyConnect によるローカル プロキシ サービスのサポートを無効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　ナビゲーション ペインで [Preferences (Part 2)] を選択します。

ステップ 3　パネル上部付近にある [Allow Local Proxy Connections] をオフにします。

最適ゲートウェイ選択

最適ゲートウェイ選択（OGS）機能を使用すると、ユーザが介入することなくインターネット トラフィックの遅延を最小限に抑えることができます。OGS を使用すると、AnyConnect では接続または再接続に最適なセキュア ゲートウェイが特定され、それが選択されます。OGS は、初回接続時または、直前の接続解除から 4 時間以上経過した後の再接続時に開始されます。

最良のパフォーマンスを実現するために、遠隔地に移動するユーザは、移動先の場所に一番近いセキュア ゲートウェイに接続します。自宅と会社では同じゲートウェイからほぼ同じ結果が得られるため、このような事例では通常セキュア ゲートウェイの切り替えは行われません。別のセキュア ゲートウェイへの接続が行われることはほとんどなく、行われるとしてもパフォーマンスの向上率が 20 % 以上の場合に限られます。

OGS はセキュリティ機能ではなく、セキュア ゲートウェイ クラスタ間またはクラスタ内部でのロードバランシングは実行されません。オプションで、エンド ユーザがこの機能の有効化 / 無効化を切り替えられるようにすることができます。

最小ラウンド トリップ時間（RTT）ソリューションでは、クライアントと他のすべてのゲートウェイとの間で RTT が最短となるセキュア ゲートウェイが選択されます。クライアントでは、経過時間が 4 時間以内の場合は常に、最後のセキュア ゲートウェイに対して再接続が行われます。ネットワーク接続の負荷やその状態の一時的変動といった要素は、インターネット トラフィックの遅延だけでなく、選択プロセスにも影響を与える場合があります。

OGS は、RTT の結果のキャッシュを維持して、その後実行する必要のある測定の数を最小限に抑えます。OGS を有効にして AnyConnect を起動すると、OGS はネットワーク情報（DNS サフィックス、DNS サーバ IP など）を取得してユーザの位置を特定します。RTT の結果は、特定した場所と一緒に OGS キャッシュに保存されます。その後 14 日間は、AC が再起動されるたびに同じ方法で場所が特定され、すでに RTT の結果が存在するかどうかが解読されます。ヘッドエンドはキャッシュに基づいて選択されるため、ヘッドエンドの再 RRT は必要ありません。この 14 日間の終了時、この場所はキャッシュから削除され、AC を再起動すると新しい RTT のセットが発生します。

選択プロセスでは、最適なサーバを特定する際プライマリ サーバにのみ問い合わせが行われます。特定後の接続アルゴリズムは次のとおりです。

1. 最適なサーバへの接続を試行する。
2. 失敗した場合は、最適なサーバのバックアップ サーバ リストに対して試行する。

3.　失敗した場合は、選択結果に応じて OGS 選択リストに残っている各サーバに対して試行する。

バックアップ サーバの詳細については、「AnyConnect プロファイル エディタの [Backup Servers]」（P.3-86）を参照してください。

最適ゲートウェイ選択に関する要件

AnyConnect は、このリリースに適合した Windows および Mac OS X オペレーティング システムを実行する VPN エンドポイントで、最適ゲートウェイ選択をサポートします。

この機能は IPv4 クライアントでのみ使用できます。

最適ゲートウェイ選択の設定

OGS のアクティブ化/非アクティブ化の制御や、エンド ユーザがこの機能そのものを制御できるようにするかどうかの指定は、AnyConnect プロファイルで行います。プロファイル エディタを使用して OGS を設定する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Enable Optimal Gateway Selection] チェックボックスをオンにして、OGS をアクティブ化します。

ステップ 3　[User Controllable] チェックボックスをオンにして、クライアント GUI にアクセスするリモート ユーザが OGS の設定を行えるようにします。

（注）　OGS が有効な場合は、この機能の設定をユーザが行えるようにすることも推奨します。OGS により選択されたゲートウェイへの接続が AnyConnect クライアントによって確立できないときには、ユーザがプロファイルから別のゲートウェイを選択できることが必要となる場合があります。

ステップ 4　VPN が一時停止してから、ゲートウェイを選択するための新たな計算が開始されるまでに要する最小の時間（単位は時間）を、[Suspension Time Threshold] パラメータに入力します。デフォルトは 4 時間です。

（注）　このしきい値は、プロファイル エディタを使用して設定できます。次の設定可能パラメータ（Performance Improvement Threshold）と組み合わせてこの値を最適化することで、最適なゲートウェイの選択と、クレデンシャルの再入力を強制する回数の削減の間の適切なバランスを見つけることができます。

ステップ 5　システムのレジューム後にクライアントから別のセキュア ゲートウェイへの再接続が行われるために必要なパフォーマンスの向上率を、[Performance Improvement Threshold] パラメータに入力します。デフォルトは 20 % です。

（注） 移行の発生回数が多く、ユーザがクレデンシャルを頻繁に再入力しなければならないような場合は、これらのしきい値の一方または両方を大きくしてください。特定のネットワークに対してこれらの値を調整すれば、最適なゲートウェイを選択することと、クレデンシャルを強制的に入力させる回数を減らすこととの間で適切なバランスを取ることができます。

クライアント GUI の起動時に OGS が有効になっている場合は、[VPN: Ready to connect] パネルの [Connect] ボタンの横に [Automatic Selection] が表示されます。この選択は変更できません。OGS を使用すると、最適なセキュア ゲートウェイが自動的に選択され、ステータス バーにその選択されたゲートウェイが表示されます。接続プロセスを開始するためには、[Select] をクリックすることが必要となる場合もあります。

この機能の設定をユーザが行えるようにした場合、選択されたセキュア ゲートウェイをユーザが手動で上書きすることができます。手順は次のとおりです。

ステップ 1　現在接続中の場合は、[Disconnect] をクリックします。

ステップ 2　[Advanced] をクリックします。

ステップ 3　[Preferences] タブを開き、[Enable Optimal Gateway Selection] をオフにします。

ステップ 4　目的のセキュア ゲートウェイを選択します。

（注） AAA が使用されている場合は、別のセキュア ゲートウェイへの移行時にエンド ユーザがそれぞれのクレデンシャルを再入力しなければならないことがあります。証明書を使用していれば、その必要はありません。

OGS とスリープ モード

エンドポイントがスリープ モードまたはハイバネーション モードに移行するときは、AnyConnect では接続が確立されているはずです。ASDM のプロファイル エディタ（[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile]）の AutoReconnect（ReconnectAfterResume）設定を有効にする必要があります。これをユーザ制御可能にした場合、デバイスをスリープにする前に AnyConnect Secure Mobility Client の [Preferences] タブで設定できます。両方を設定すると、デバイスがスリープから復帰したときに、AC は再接続試行用に選択したヘッドエンドを使用して、自動的に OGS を実行します。

OGS とプロキシ検出

自動プロキシ検出が設定されている場合は、OGS は実行できません。また、プロキシ自動設定（PAC）ファイルを設定した状態でも、動作しません。

スクリプトの作成および展開

AnyConnect では、次のイベントが発生したときに、スクリプトをダウンロードして実行できます。

- セキュリティ アプライアンスで新しいクライアント VPN セッションが確立された。このイベントによって起動するスクリプトを *OnConnect* スクリプトと呼びます。スクリプトには、このファイル名プレフィックスが必要です。
- セキュリティ アプライアンスでクライアント VPN セッションが切断された。このイベントによって起動するスクリプトを *OnDisconnect* スクリプトと呼びます。スクリプトには、このファイル名プレフィックスが必要です。

これにより、Trusted Network Detection によって開始された新しいクライアント VPN セッションが確立すると、OnConnect スクリプトが起動します（このスクリプトを実行する要件が満たされている場合）。ネットワーク切断後に永続的な VPN セッションが再接続されても、OnConnect スクリプトは起動しません。

この機能には次のような使用例があります。

- VPN 接続時にグループ ポリシーを更新する。
- VPN 接続時にネットワーク ドライブをマッピングし、接続解除後にマッピングを解除する。
- VPN 接続時にサービスにログインし、接続解除後にログオフする。

AnyConnect は、WebLaunch の起動中およびスタンドアロン起動中でのスクリプトの起動をサポートしています。

ここでの説明は、スクリプトの作成方法と、ターゲット エンドポイントのコマンドラインからスクリプトを実行し、テストする方法についての知識があることを前提としています。

（注） AnyConnect のソフトウェア ダウンロード サイトでは、サンプル スクリプトがいくつか提供されています。これらを確認する場合は、単なるサンプルであることに留意してください。これらのサンプル スクリプトは、スクリプトを実行するために必要なローカル コンピュータの要件を満たしていない場合があります。また、ご使用のネットワークおよびユーザのニーズに応じてカスタマイズしてからでないと使用できません。シスコでは、サンプル スクリプトまたはユーザ作成スクリプトはサポートしていません。

この項では、次のトピックについて取り上げます。

スクリプトの要件と制限

次のスクリプトの要件と制限事項に留意してください。

サポートされるスクリプトの数

AnyConnect は、1 つの OnConnect スクリプトおよび 1 つの OnDisconnect スクリプトのみを実行します。ただし、これらのスクリプトが別のスクリプトを起動する場合があります。

スクリプト言語

クライアントでは、スクリプトを特定の言語で作成する必要はありません。ただし、スクリプトを実行可能なアプリケーションが、クライアント コンピュータにインストールされている必要があります。クライアントでスクリプトを起動するためには、このスクリプトがコマンドラインから実行可能であることが必要です。

Windows Mobile 用スクリプト

AnyConnect がサポートするすべての Microsoft Windows プラットフォーム、Mac OS X プラットフォーム、および Linux プラットフォームで、スクリプトの起動がサポートされます。Microsoft Windows Mobile では、スクリプト言語のネイティブ サポートはありませんが、スクリプト ファイル名プレフィックスとディレクトリ要件を使用してコンパイルすれば、OnConnect アプリケーションと OnDisconnect アプリケーションを作成して自動的に実行できます。

Windows セキュリティ環境によるスクリプトの制限

Microsoft Windows 上の AnyConnect では、ユーザが Windows にログインして VPN セッションを確立した後でないと、スクリプトを起動できません。そのため、ユーザのセキュリティ環境に伴う制限が、これらのスクリプトに適用されます。スクリプトが実行できる機能は、ユーザが起動権限を持つ機能に限られます。AnyConnect は、Windows でスクリプトを実行中は CMD ウィンドウを非表示にします。したがって、テストの目的で、.bat ファイル内のメッセージを表示するスクリプトを実行しても機能しません。

スクリプトの有効化

デフォルトでは、クライアントによってスクリプトが起動することはありません。AnyConnect プロファイルの EnableScripting パラメータを使用して、スクリプトを有効にしてください。これにより、クライアントではスクリプトが存在する必要がなくなります。

クライアント GUI の終了

クライアント GUI を終了しても、必ずしも VPN セッションは終了しません。OnDisconnect スクリプトは、セッションが終了した後で実行されます。

64 ビット Windows でのスクリプトの実行

AnyConnect クライアントは、32 ビット アプリケーションです。Windows 7 x64 および Windows Vista SP2 x64 などの 64 ビット Windows バージョンで動作させる場合は、バッチ スクリプトを実行するときに、32 ビット バージョンの cmd.exe を使用します。

32 ビットの cmd.exe では、64 ビットの cmd.exe でサポートされているコマンドの一部が欠けているため、一部のスクリプトについては、サポートされていないコマンドの実行を試行したときにスクリプトの実行が停止したり、一部実行されてから停止したりする場合があります。たとえば、64 ビットの cmd.exe でサポートされている **msg** コマンドは、32 ビット バージョンの Windows 7（%WINDIR%\SysWOW64 に含まれる）では理解されない場合があります。

そのため、スクリプトを作成する場合は、32 ビットの cmd.exe でサポートされているコマンドを使用してください。

スクリプトの作成、テスト、および展開

AnyConnect スクリプトを展開する手順は次のとおりです。

ステップ 1　AnyConnect が起動したスクリプトが実行されるオペレーティング システムのタイプに基づいて、スクリプトの作成とテストを行います。

（注） Microsoft Windows コンピュータで作成されたスクリプトの行末コードは、Mac OS および Linux で作成されたスクリプトの行末コードとは異なります。そのため、ターゲットのオペレーティング システムでスクリプトを作成し、テストする必要があります。ネイティブ オペレーティング システムのコマンドラインからスクリプトを正しく実行できない場合は、AnyConnect でも正しく実行できません。

ステップ 2　次のいずれかを実行して、スクリプトを展開します。

- ASDM を使用して、スクリプトをバイナリ ファイルとして ASA にインポートします。[Network (Client) Access] > [AnyConnect Customization/Localization] > [Script] を選択します。

  （注） Microsoft Windows Mobile では、このオプションはサポートされません。このオペレーティング システム用のスクリプトを展開するには、企業のソフトウェア展開システムを使用してください。

  ASDM バージョン 6.3 以降を使用している場合、ASA では、ファイルをスクリプトとして識別できるように、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、セキュリティ アプライアンスは、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、*scripts_* プレフィックスを削除し、*OnConnect* プレフィックスまたは *OnDisconnect* プレフィックスをそのまま残します。たとえば、*myscript.bat* スクリプトをインポートする場合、スクリプトは、セキュリティ アプライアンス上では *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。

  6.3 よりも前の ASDM バージョンを使用している場合には、次のプレフィックスでスクリプトをインポートする必要があります。

  - scripts_OnConnect
  - scripts_OnDisconnect

  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。

- 企業のソフトウェア展開システムを使用して、スクリプトを実行する VPN エンドポイントにスクリプトを手動で展開します。

  この方式を使用する場合は、次のファイル名プレフィックスを使用します。

  - OnConnect
  - OnDisconnect

  表 3-8 に示すディレクトリにスクリプトをインストールします。

表 3-8　スクリプトの所定の場所

OS	ディレクトリ
Microsoft Windows 7 および Microsoft Vista	%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script
Microsoft Windows XP	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Script
Linux （Linux では、User、Group、Other にファイルの実行権限を割り当てます）	/opt/cisco/anyconnect
Mac OS X	/opt/cisco/anyconnect/script

スクリプトに関する AnyConnect プロファイルの設定

クライアント プロファイルでスクリプトを有効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　ナビゲーション ペインで [Preferences (Part 2)] を選択します。

ステップ 3　[Enable Scripting] をオンにします。クライアントでは、VPN 接続の接続時または接続解除時にスクリプトが起動します。

ステップ 4　[User Controllable] をオンにして、On Connect スクリプトおよび OnDisconnect スクリプトの実行をユーザが有効または無効にすることができるようにします。

ステップ 5　[Terminate Script On Next Event] をオンにして、スクリプト処理可能な別のイベントへの移行が発生した場合に、実行中のスクリプト プロセスをクライアントが終了できるようにします。たとえば、VPN セッションが終了すると、クライアントでは実行中の On Connect スクリプトが終了し、AnyConnect で新しい VPN セッションが開始すると、実行中の OnDisconnect スクリプトが終了します。Microsoft Windows 上のクライアントでは OnConnect スクリプトまたは OnDisconnect スクリプトによって起動した任意のスクリプト、およびその従属スクリプトもすべて終了します。Mac OS および Linux 上のクライアントでは、OnConnect スクリプトまたは OnDisconnect スクリプトのみ終了し、子スクリプトは終了しません。

ステップ 6　[Enable Post SBL On Connect Script] をオンにして（デフォルトでオン）、SBL で VPN セッションが確立された場合にクライアントにより OnConnect スクリプトが（存在すれば）起動するようにします。

（注）　必ずクライアント プロファイルを ASA のグループ ポリシーに追加し、それを VPN エンドポイントにダウンロードしてください。

スクリプトのトラブルシューティング

スクリプトの実行に失敗した場合は、次のようにして問題を解決してください。

ステップ 1　スクリプトに、`OnConnect` または `OnDisconnect` のプレフィックス名が付いていることを確認します。表 3-8 には、各オペレーティング システムの所定のスクリプト ディレクトリが記載されています。

ステップ 2　スクリプトをコマンドラインから実行してみます。コマンドラインから実行できないスクリプトは、クライアントでも実行できません。コマンドラインでスクリプトの実行に失敗する場合は、スクリプトを実行するアプリケーションがインストールされていることを確認し、そのオペレーティング システムでスクリプトを作成し直してください。

ステップ 3　VPN エンドポイントのスクリプト ディレクトリ内に OnConnect スクリプトと OnDisconnect スクリプトがそれぞれ 1 つだけ存在することを確認します。最初の ASA で OnConnect スクリプトがダウンロードされ、その後の接続で次の ASA により別のファイル名拡張子を持つ OnConnect スクリプトがダウンロードされる、クライアントでは不要なスクリプトが実行される可能性があります。スクリプト パスに複数の OnConnect スクリプトまたは OnDisconnect スクリプトが含まれており、かつスクリプトの展開に ASA を使用している場合は、スクリプト ディレクトリ内のファイルを削除し、VPN セッションを再確立します。スクリプト パスに複数の OnConnect スクリプトまたは OnDisconnect スクリプトが含まれており、かつ手動展開を使用している場合は、不要なスクリプトを削除し、AnyConnect VPN セッションを再確立します。

ステップ 4　オペレーティング システムが Linux の場合は、スクリプト ファイルに実行権限が設定されていることを確認します。

ステップ 5　クライアント プロファイルでスクリプトが有効になっていることを確認します。

認証タイムアウト コントロール

デフォルトでは、AnyConnect は接続試行を終了するまでに、セキュア ゲートウェイからの認証を最大 12 秒間待ちます。その時間が経過すると、認証がタイムアウトになったことを示すメッセージが表示されます。次の項の説明に従って、このタイマーの値を変更します。

認証タイムアウト コントロールに関する要件

AnyConnect は、AnyConnect がサポートしているすべての OS 上でこの機能をサポートしています。

この機能をサポートするためには、AnyConnect Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition ライセンスのどちらかが必要です。

認証タイムアウトの設定

AnyConnect が接続の試行を終了しないでセキュア ゲートウェイでの認証を待機している秒数を変更する手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　ナビゲーション ペインで [Preferences (Part 2)] を選択します。

ステップ 3　[Authentication Timeout Values] テキスト ボックスに 10 ～ 120 の範囲で秒数を入力します。

プロキシ サポート

ここでは、プロキシ サポート拡張機能の使用方法について説明します。

ブラウザのプロキシ設定を無視するためのクライアントの設定

AnyConnect プロファイルでは、ユーザの PC 上で Microsoft Internet Explorer のプロキシ設定が無視されるようにポリシーを指定できます。これは、プロキシ設定によってユーザが企業ネットワークの外部からトンネルを確立できない場合に役立ちます。

（注）　常時接続機能が有効な場合、プロキシ経由の接続はサポートされません。そのため、常時接続を有効にした場合は、プロキシ設定を無視するようにクライアントを設定する必要はありません。

AnyConnect で Internet Explorer のプロキシ設定が無視されるようにする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Preferences (Part 2)] ペインに移動します。

ステップ 3　[Proxy Settings] ドロップダウン リストで、[Ignore Proxy] を選択します。[Ignore Proxy] を選択すると、クライアントはすべてのプロキシ設定を無視します。ASA に到達するプロキシには、何のアクションも実行されません。

（注）　AnyConnect では、プロキシの設定として [Override] はサポートしていません。

プライベート プロキシ

トンネルを確立した後、グループ ポリシー内に設定されたプライベート プロキシ設定をブラウザにダウンロードするように、グループ ポリシーを設定できます。VPN セッションが終了すると、設定は元の状態に復元されます。

プライベート プロキシの要件

AnyConnect Essentials ライセンスは、この機能の最小 ASA ライセンス アクティブ化要件です。

AnyConnect は、以下が動作するコンピュータ上でこの機能をサポートします。

- Windows 上の Internet Explorer
- Mac OS 上の Safari

グループ ポリシーを設定してプライベート プロキシをダウンロード

プロキシ設定を設定するには、セキュリティ アプライアンスで ASDM セッションを確立し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [Browser Proxy] の順に選択します。6.3(1) より前の ASDM バージョンでは、このオプションは [IE Browser Proxy] として表示されます。しかし、現在 AnyConnect は、使用する ASDM バージョンに関係なく、プライベート プロキシの設定を Internet Explorer に限定していません。

プロキシを使用しないパラメータが有効の場合、セッションの間、ブラウザからプロキシ設定が削除されます。

Internet Explorer の [Connections] タブのロック

ある条件下では、AnyConnect によって Internet Explorer の [Tools] > [Internet Options] > [Connections] タブが非表示にされます。このタブが表示されている場合、ユーザはプロキシ情報を設定できます。このタブを非表示にすると、ユーザが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックは接続解除すると反転され、このタブに関する管理者定義のポリシーの方が優先されます。このロックは、次のいずれかの条件で行われます。

- ASA の設定で、[Connections] タブのロックが指定されている。
- ASA の設定で、プライベート側プロキシが指定されている。
- Windows のグループ ポリシーにより、以前に [Connections] タブがロックされている（**no lockdown** ASA グループ ポリシー設定の上書き）。

グループ ポリシーで、ASA がプロキシのロックダウンを許可したり、許可しないように設定できます。ASDM を使用してこれを設定する手順は次のとおりです。

ステップ 1　[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。[Edit Internal Group Policy] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Advanced] > [Browser Proxy] に移動します。[Proxy Server Policy] ペインが表示されます。

ステップ 4　[Proxy Lockdown] をクリックして、その他のプロキシ設定を表示します。

ステップ 5　プロキシのロックダウンを有効にして、AnyConnect のセッション中は [Internet Explorer Connections] タブを非表示にするには、[Inherit] をオフにして [Yes] を選択します。または、プロキシのロックダウンを無効にして、AnyConnect のセッション中は [Internet Explorer Connections] タブを表示するには、[No] を選択します。

ステップ 6　[OK] をクリックして、プロキシ サーバ ポリシーの変更を保存します。

ステップ 7　[Apply] をクリックして、グループ ポリシーの変更を保存します。

クライアントレス サポートのためのプロキシ自動設定ファイルの生成

一部のバージョンの ASA では、AnyConnect セッションが確立された後も、プロキシ サーバを経由するクライアントレス ポータル アクセスを許可するために追加の AnyConnect 設定が必要です。AnyConnect では、この設定が行われるように、プロキシ自動設定（PAC）ファイルを使用してクライアント側プロキシ設定が修正されます。AnyConnect でこのファイルが生成されるのは、ASA でプライベート側プロキシ設定が指定されていない場合のみです。

Windows RDP セッションによる VPN セッションの起動

Windows リモート デスクトップ プロトコル（RDP）を使用して、ユーザが Cisco AnyConnect Secure Mobility Client を実行するコンピュータにログインして、RDP セッションからセキュア ゲートウェイへの VPN 接続を作成するように許可できます。この機能が正しく動作するには、スプリット トンネリング VPN 設定が必要です。

デフォルトでは、他のローカル ユーザがログインしていない場合に限り、ローカルにログインしたユーザが VPN 接続を確立できます。ユーザがログアウトすると VPN 接続は終了し、VPN 接続中に別のローカル ログインが行われると接続は切断されます。VPN 接続中のリモート ログインおよびログアウトは制限されません。

（注） この機能を使用すると、AnyConnect では、VPN 接続を確立したユーザがログオフした時点でその VPN 接続が解除されます。接続がリモート ユーザによって確立された場合は、そのリモート ユーザがログオフした時点で VPN 接続は終了します。

[Windows Logon Enforcement] に対しては次の設定を使用できます。

- [Single Local Logon] : VPN 接続全体で、ログインできるローカル ユーザは 1 人だけです。この設定では、ローカル ユーザは 1 人以上のリモート ユーザがクライアント PC にログインしている場合でも VPN 接続を確立できますが、VPN 接続が排他的トンネリング用に設定されている場合は、VPN 接続のクライアント PC ルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログオンが接続解除されるかどうかは、VPN 接続のルーティング設定によって決まります。SingleLocalLogin 設定は、VPN 接続を介した企業ネットワークからのリモート ユーザ ログインに対しては影響を与えません。
- [SingleLogon] : VPN 接続の全体で、ログインできるユーザは 1 人だけです。1 人以上のユーザがログインして、ローカルまたはリモートで VPN 接続を確率した場合、接続は許可されません。ローカルまたはリモートで第 2 のユーザがログインすると、その VPN 接続は終了します。

（注） SingleLogon 設定を選択した場合、VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

クライアント プロファイルの [Windows VPN Establishment] の設定では、AnyConnect が実行されているコンピュータにリモート ログインしたユーザが VPN 接続を確立する場合のクライアントの動作が指定されます。次の値が可能です。

- [Local Users Only] : リモート ログインしたユーザは、VPN 接続を確立できません。AnyConnect クライアント バージョン 2.3 以前の動作はこの方式でした。

- [Allow Remote Users]：リモート ユーザは VPN 接続を確立できます。ただし、設定された VPN 接続ルーティングによってリモート ユーザが接続解除された場合は、リモート ユーザがクライアント コンピュータに再アクセスできるように VPN 接続が終了します。リモート ユーザが VPN セッションを終了せずに RDP セッションを接続解除するには、VPN を確立した後、90 秒間待つ必要があります。

（注） 現在 Vista では、Start Before Logon（SBL）中にプロファイルの [Windows VPN Establishment] 設定が適用されることはありません。AnyConnect では、VPN 接続を確立したのがログイン前のリモート ユーザかどうかの判定は行われません。そのため、[Windows VPN Establishment] の設定が [*Local Users Only*] でも、リモート ユーザが SBL を介して VPN 接続を確立することは可能です。

Windows RDP セッションから AnyConnect セッションを有効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Preferences] ペインに移動します。

ステップ 3　Windows ログイン実行方式を選択します。

- [Single Local Logon]：VPN 接続全体で、ログインできるローカル ユーザは 1 人だけです。
- [Single Logon]：VPN 接続全体で、ログインできるユーザは 1 人だけです。

ステップ 4　リモート ログインしたユーザが VPN 接続を確立する場合のクライアントの動作を指定する Windows ログイン実行方式を選択します。

- [Local Users Only]：リモート ログインしたユーザは、VPN 接続を確立できません。
- [Allow Remote Users]：リモート ユーザは VPN 接続を確立できます。

（注） 現在 Vista では、Start Before Logon（SBL）中にプロファイルの [Windows VPN Establishment] 設定が適用されることはありません。

L2TP または PPTP を介した AnyConnect

一部の国の ISP では、L2TP トンネリング プロトコルおよび PPTP トンネリング プロトコルのサポートが必要です。

セキュア ゲートウェイを宛先としたトラフィックを PPP 接続上で送信する場合、AnyConnect では外部トンネルが生成したポイントツーポイント アダプタが使用されます。PPP 接続上で VPN トンネルを確立する場合、クライアントでは ASA より先を宛先としてトンネリングされたトラフィックから、この ASA を宛先とするトラフィックが除外される必要があります。除外ルートを特定するかどうかや、除外ルートを特定する方法を指定する場合は、AnyConnect プロファイルの [PPP Exclusion] 設定を使用します。除外ルートは、セキュアでないルートとして AnyConnect GUI の [Route Details] 画面に表示されます。

ここでは、PPP 除外の設定方法について説明します。

L2TP または PPTP を介した AnyConnect の設定

デフォルトでは、[PPP Exclusion] は無効です。プロファイルで PPP 除外を有効にする手順は次のとおりです。

ステップ 1　ASDM からプロファイル エディタを起動します（「AnyConnect プロファイルの設定と編集」（P.3-9）を参照）。

ステップ 2　[Preferences (Part 2)] ペインに移動します。

ステップ 3　[PPP Exclusion] でその方式を選択します。このフィールドで [User Controllable] をオンにすると、ユーザには次の設定が表示され、ユーザはそれらを変更することができます。

- [Automatic] : PPP 除外を有効にします。AnyConnect では自動的に、PPP サーバの IP アドレスが使用されます。この値は、自動検出による IP アドレスの取得に失敗すした場合にのみ変更するよう、ユーザに指示してください。
- [Override] : 同様に PPP 除外を有効にします。自動検出で PPP サーバの IP アドレスを取得できず、PPPExclusion の UserControllable 値が true である場合は、次項の説明に従ってこの設定を使用するよう、ユーザに指示してください。
- [Disabled] : PPP 除外は適用されません。

ステップ 4　[PPP Exclusion Server IP] フィールドに、PPP 除外に使用されるセキュリティ ゲートウェイの IP アドレスを入力します。このフィールドで [User Controllable] をオンにすると、ユーザにこの IP アドレスが表示され、ユーザをそれを変更することができます。

ユーザによる PPP 除外の上書き

自動検出が機能しない場合に、PPP 除外をユーザ設定可能に設定すると、ユーザはローカル コンピュータ上で AnyConnect プリファレンス ファイルを編集することにより、これらの設定を上書きすることができます。次の手順では、その方法について説明します。

ステップ 1　メモ帳などのエディタを使用して、プリファレンス XML ファイルを開きます。

このファイルは、ユーザのコンピュータ上で次のいずれかのパスにあります。

- Windows : %LOCAL_APPDATA%\Cisco\Cisco AnyConnect VPN Client\preferences.xml。次に例を示します。
  - Windows Vista : C:\Users*username*\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml
  - Windows XP : C:\Documents and Settings**username**\Local Settings\Application Data\Cisco\Cisco AnyConnect VPN Client\preferences.xml
- Mac OS X : /Users/username/.anyconnect
- Linux : /home/username/.anyconnect

ステップ 2　PPPExclusion の詳細を `<ControllablePreferences>` の下に挿入して、Override 値と PPP サーバの IP アドレスを指定します。アドレスは、完全な形式の IPv4 アドレスにする必要があります。次に例を示します。

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
```

```
</ControllablePreferences>
</AnyConnectPreferences>
```

ステップ 3　ファイルを保存します。

ステップ 4　AnyConnect を終了し、リスタートします。

AnyConnect VPN プロファイル エディタのパラメータに関する説明

ここでは、プロファイル エディタのさまざまなペインに表示されるすべての設定について説明します。

AnyConnect プロファイル エディタ、プリファレンス（パート 1）

[Use Start Before Logon]（Windows のみ）：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、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。認証後、ログイン ダイアログボックスが表示され、ユーザは通常どおりログインします。SBL では、ログイン スクリプト、パスワードのキャッシュ、ネットワーク ドライブからローカル ドライブへのマッピングなどの使用を制御できます。

[Show Pre-connect Message]：初めて接続を試行するユーザに対してメッセージを表示します。たとえば、スマートカードをリーダーに必ず挿入するようユーザに知らせることもできます。事前接続メッセージの設定または変更の詳細については、「デフォルトの AnyConnect の英語メッセージの変更」（P.12-15）を参照してください。

[Certificate Store]：AnyConnect がどの証明書ストアで証明書を保存し、読み取るかを制御します。Windows では、ローカル マシン用の証明書ストアと現在のユーザ用の証明書ストアが別々に用意されます。ほとんどの場合、デフォルト設定（All）が適しています。変更が必要となる特別な理由またはシナリオ要件がある場合を除いて、この設定は変更しないでください。

- [All]：（デフォルト）証明書は両方のストアに保存されています。
- [Machine]：マシン ストアを使用します。
- [User]：ユーザ証明書ストアを使用します。

[Certificate Store Override]：Windows のマシン証明書ストアで証明書を検索するよう AnyConnect を設定することができます。これは、証明書がマシン ストアにあり、ユーザにマシンの管理者権限がない場合に役立ちます。

[Auto Connect on Start]：AnyConnect の起動時に、AnyConnect プロファイルで指定されたセキュア ゲートウェイまたはクライアントが最後に接続していたゲートウェイとの VPN 接続が自動的に確立されます。

[Minimize On Connect]：VPN 接続の確立後、AnyConnect GUI が最小化されます。

[Local LAN Access]：ASA への VPN セッション中にリモート コンピュータへ接続したローカル LAN に対してユーザが無制限にアクセスできるようになります。

（注）　[Local LAN Access] を有効にすると、パブリック ネットワークからユーザ コンピュータを経由して、企業ネットワークにセキュリティの脆弱性が生じる可能性があります。代替手段として、セキュリティ アプライアンス（バージョン 8.3(1) 以降）で、デフォルト グループ ポリシーに含まれている AnyConnect クライアント ローカル印刷ファイアウォール ルールを使用した SSL クライアント ファイアウォールを展開するように設定することもできます。このファイアウォール ルールを有効にするには、このエディタ [Preferences (Part 2)] で [Automatic VPN Policy]、[Always On]、および [Allow VPN Disconnect] も有効にする必要があります。

[Auto Reconnect]：接続が解除された場合、AnyConnect により VPN 接続の再確立が試行されます（デフォルトで有効）。[Auto Reconnect] を有効にすると、接続解除の原因にかかわらず、再接続は試行されません。

自動再接続の動作は次のとおりです。

- [DisconnectOnSuspend]（デフォルト）：AnyConnect では、システムの一時停止時に VPN セッションに割り当てられたリソースが解放され、システムのレジューム後も再接続は試行されません。
- [ReconnectAfterResume]：接続が解除された場合、AnyConnect により VPN 接続の再確立が試行されます。

（注）　AnyConnect 2.3 よりも前までは、システムの一時停止に対するデフォルトの動作として、VPN セッションに割り当てられたリソースを保持し、システムのレジューム後に VPN 接続を再確立していました。この動作を維持する場合は、自動再接続の動作として **ReconnectAfterResume** を選択します。

[Auto Update]：オンにすると、クライアントの自動アップデートが有効になります。[User Controllable] チェックボックスをオンにすると、クライアントのこの設定を無効にできます。

[RSA Secure ID Integration]（Windows のみ）：ユーザが RSA とどのようにインタラクトするかを制御します。デフォルトでは、AnyConnect により RSA インタラクションの適切な方式が指定されます（自動設定）。

- [Automatic]：ソフトウェア トークンおよびハードウェア トークンが許可されます。
- [Software Token]：ソフトウェア トークンのみ許可されます。
- [Hardware Token]：ハードウェア トークンのみ許可されます。

[Windows Logon Enforcement]：リモート デスクトップ プロトコル（RDP）からの VPN セッションの確立を許可します。スプリット トンネリングはグループ ポリシーで設定する必要があります。VPN 接続を確立したユーザがログオフすると、その VPN 接続は AnyConnect により解除されます。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。

- [Single Local Logon]：VPN 接続全体で、ログインできるローカル ユーザは 1 人だけです。クライアント PC に複数のリモート ユーザがログインしている場合でも、ローカル ユーザが VPN 接続を確立することはできます。
- [Single Logon]：VPN 接続全体で、ログインできるユーザは 1 人だけです。VPN 接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN 接続中にローカルまたはリモートで第 2 のユーザがログインすると、VPN 接続が終了します。VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

[Windows VPN Establishment]：クライアント PC にリモート ログインしたユーザが VPN 接続を確立した場合の AnyConnect の動作を決定します。次の値が可能です。

- [Local Users Only]：リモート ログインしたユーザは、VPN 接続を確立できません。これは、以前のバージョンの AnyConnect と同じ機能です。
- [Allow Remote Users]：リモート ユーザは VPN 接続を確立できます。ただし、設定された VPN 接続ルーティングによってリモート ユーザが接続解除された場合は、リモート ユーザがクライアント PC に再アクセスできるように、VPN 接続が終了します。リモート ユーザが VPN 接続を終了せずにリモート ログイン セッションを接続解除するには、VPN を確立した後、90 秒間待つ必要があります。

（注）　現在 Vista では、Start Before Logon（SBL）中にプロファイルの [Windows VPN Establishment] 設定が適用されることはありません。AnyConnect では、VPN 接続を確立したのがログイン前のリモート ユーザかどうかの判定は行われません。そのため、[Windows VPN Establishment] の設定が [Local Users Only] でも、リモート ユーザが SBL を介して VPN 接続を確立することは可能です。

- [IP Protocol Supported]：IPv4 アドレスおよび IPv6 アドレスの両方で AnyConnect を使用して ASA に接続しようとしているクライアントの場合、AnyConnect は接続の開始に際してどの IP プロトコルを使用するか決定する必要があります。デフォルトで、AnyConnect は最初に IPv4 を使用して接続しようとします。接続が成功しない場合、IPv6 を使用して接続を開始しようとします。

  このフィールドでは、最初の IP プロトコルとフォールバックの順序を設定します。

  - [IPv4]：ASA に対して IPv4 接続のみ可能です。
  - [IPv6]：ASA に対して IPv6 接続のみ可能です。
  - [IPv4, IPv6]：最初に ASA に IPv4 接続しようとします。クライアントが IPv4 を使用して接続できない場合、IPv6 接続をしようとします。
  - [IPv6, IPv4]：最初に ASA に IPv6 接続しようとします。クライアントが IPv6 を使用して接続できない場合、IPv4 接続をしようとします。

（注）　IPv4 から IPv6、IPv6 から IPv4 プロトコルへのフェールオーバーも VPN セッション中に行うことができます。プライマリ IP プロトコルが失われると、可能な場合に、セカンダリ IP プロトコルを介して VPN セッションが再確立されます。

このペインに表示されるクライアント機能に関するより詳細な設定情報については、次の各項を参照してください。

- 「Windows 7 システムおよび Windows Vista システムでの Start Before Logon（PLAP）の設定」（P.3-16）
- 「証明書の失効通知の設定」（P.3-51）
- 「自動再接続の設定」（P.3-66）
- 「Windows RDP セッションによる VPN セッションの起動」（P.3-77）

AnyConnect プロファイル エディタ、プリファレンス（パート 2）

[Disable Certificate Selection]：クライアントによる自動証明書選択を無効にし、ユーザに対して認証証明書を選択するためのプロンプトを表示します。

[Allow Local Proxy Connections]：デフォルトでは、Windows ユーザは AnyConnect でローカル PC 上のトランスペアレントまたは非トランスペアレントのプロキシを介して VPN セッションを確立するようになっています。次に示すのは、透過的なプロキシ サービスを実現する要素の一例です。

- 一部のワイヤレス データ カードから入手できるアクセラレーション ソフトウェア
- 一部のアンチウイルス ソフトウェア上のネットワーク コンポーネント

ローカル プロキシ接続のサポートを無効にする場合は、このパラメータをオフにします。

[Proxy Settings]：リモート コンピュータ上の Microsoft Internet Explorer または Mac Safari のプロキシ設定を無視するように、AnyConnect プロファイルでポリシーを指定できます。これは、プロキシ設定によってユーザが企業ネットワークの外部からトンネルを確立できない場合に役立ちます。ASA 上のプロキシ設定と併用します。

- [Native]：クライアントは、クライアントで設定されたプロキシ設定および Internet Explorer で設定されたプロキシ設定の両方を使用します。ネイティブ OS プロキシ設定（Windows の MSIE に設定されたものなど）が使用され、グローバル ユーザ プリファレンスで設定されたプロキシ設定はこれらのネイティブ設定の先頭に追加されます。
- [Ignore Proxy]：ユーザ コンピュータ上の Microsoft Internet Explorer または Mac Safari のプロキシ設定が無視されます。ASA に到達するプロキシには、何のアクションも実行されません。
- [Override]（サポートされていません）

[Enable Optimal Gateway Selection]：AnyConnect では、ラウンド トリップ時間（RTT）に基づいて接続または再接続に最適なセキュア ゲートウェイが特定され、それが選択されます。これにより、ユーザが介入することなくインターネット トラフィックの遅延を最小限に抑えることができます。クライアント GUI の [Connection] タブにある [Connect To] ドロップダウン リストには [Automatic Selection] が表示されます。

- [Suspension Time Threshold]（単位は時間）：現在のセキュア ゲートウェイへの接続が解除されてから、別のセキュア ゲートウェイに再接続するまでの経過時間。ユーザが対応するゲートウェイ間の移行が極端に多い場合は、この時間を長くします。
- [Performance Improvement Threshold]（単位は %）：クライアントが別のセキュア ゲートウェイに接続する際の基準となるパフォーマンス向上率。デフォルトは 20 % です。

（注）　AAA が使用されている場合は、別のセキュア ゲートウェイへの移行時にユーザがそれぞれのクレデンシャルを再入力しなければならないことがあります。この問題は、証明書を使用すると解消されます。

[Automatic VPN Policy]（Windows および Mac のみ）：信頼ネットワーク ポリシーおよび非信頼ネットワーク ポリシーに従って VPN 接続を開始または停止することが必要な状況を自動で管理します。無効の場合、VPN 接続の開始および停止は手動でのみ行うことができます。

（注）　[Automatic VPN Policy] の設定にかかわらず、ユーザは VPN 接続を手動で制御できます。

- [Trusted Network Policy]：ユーザが企業ネットワークの中（信頼ネットワーク）に存在する場合、AnyConnect により VPN 接続が自動的に解除されます。
  - [Disconnect]：信頼ネットワークが検出されると VPN 接続が解除されます。
  - [Connect]：信頼ネットワークが検出されると VPN 接続が開始されます。
  - [Do Nothing]：信頼ネットワークでは動作はありません。[Trusted Network Policy] および [Untrusted Network Policy] を共に [Do Nothing] に設定すると、Trusted Network Detection は無効となります。

  - [Pause]：ユーザが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、AnyConnect は VPN セッションを接続解除するのではなく、一時停止します。ユーザが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。

- [Untrusted Network Policy]：ユーザが企業ネットワークの外（非信頼ネットワーク）に存在する場合、AnyConnect により VPN 接続が自動的に開始されます。この機能を使用すると、ユーザが信頼ネットワークの外にいるときに VPN 接続を開始することによって、セキュリティ意識を高めることができます。
  - [Connect]：非信頼ネットワークが検出されると VPN 接続が開始されます。
  - [Do Nothing]：非信頼ネットワークが検出されると VPN 接続が開始されます。このオプションを選択すると、VPN 常時接続は無効となります。[Trusted Network Policy] および [Untrusted Network Policy] を共に [Do Nothing] に設定すると、Trusted Network Detection は無効となります。
- [Trusted DNS Domains]：クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列）。*.cisco.com などがこれに該当します。DNS サフィックスでは、ワイルドカード（*）がサポートされます。
- [Trusted DNS Servers]：クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サーバ アドレス（カンマ区切りの文字列）。たとえば、192.168.1.2, 2001:DB8::1 です。
- [Always On]：対応している Windows または Mac OS X オペレーティング システムのいずれかを実行しているコンピュータにユーザがログインした場合、AnyConnect が VPN へ自動的に接続するかどうかを判断します。この機能を使用すると、コンピュータが信頼ネットワーク内に存在しない場合にはインターネット リソースへのアクセスを制限することによってセキュリティ上の脅威からコンピュータを保護するという企業ポリシーが適用されます。グループ ポリシーおよびダイナミック アクセス ポリシーで VPN 常時接続パラメータを設定すると、この設定を上書きすることができます。これにより、ポリシーの割り当てに使用される一致基準に従って例外を指定できます。AnyConnect ポリシーでは VPN 常時接続が有効になっているが、ダイナミック アクセス ポリシーまたはグループ ポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループ ポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。

  [Always On] チェックボックスをオンにした後、[Allow VPN Disconnect] チェックボックスをオンにできます。
- [Allow VPN Disconnect]：AnyConnect で VPN 常時接続セッション用の [Disconnect] ボタンが表示されるようにするかどうかを指定します。VPN 常時接続セッションのユーザは、[Disconnect] をクリックすることが必要になる場合があるため、次のような問題に対処できるよう代替セキュア ゲートウェイを選択することができます。
  - 現在の VPN セッションに関するパフォーマンスの問題。
  - VPN セッションが中断した後に生じる再接続の問題。

注意　[Disconnect] ボタンをクリックすると、すべてのインターフェイスがロックされます。これにより、データの漏洩を防ぐことができるほか、VPN セッションの確立には必要のないインターネット アクセスからコンピュータを保護することができます。上述した理由により、[Disconnect] ボタンを無効にすると、VPN アクセスが妨害または阻止されることがあります。

この機能の詳細については、「VPN 常時接続用の [Disconnect] ボタン」（P.3-28）を参照してください。

[AllowVPN Disconnect] を有効にした後、[Connect Failure Policy]、[Allow Captive Portal Remediation]、および [Apply Last VPN Local Resource Rules] を設定できます。

- [Connect Failure Policy] : AnyConnect が VPN セッションを確立できない場合（ASA が到達不能の場合など）に、コンピュータがインターネットにアクセスできるようにするかどうかを指定します。このパラメータは、VPN 常時接続が有効な場合にのみ適用されます。

注意 AnyConnect が VPN セッションの確立に失敗した場合は、接続障害クローズド ポリシーによりネットワーク アクセスは制限されます。AnyConnect では、キャプティブ ポータルの大半が検出されます。ただし、キャプティブ ポータルを検出できない場合は、接続障害クローズド ポリシーによりネットワーク接続は制限されます。接続障害ポリシーの設定を行う場合は必ず、事前に「VPN 常時接続に関する接続障害ポリシー」（P.3-29）を一読してください。

  - [Closed] : VPN が到達不能の場合にネットワーク アクセスを制限します。この設定の目的は、エンドポイントを保護するプライベート ネットワーク内のリソースが使用できない場合に、企業の資産をネットワークに対する脅威から保護することにあります。
  - [Open] : VPN が到達不能の場合でもネットワーク アクセスを許可します。

    [Connect Failure Policy] : 接続障害ポリシーを Closed にすると、次の設定を行うことができます。
  - [Allow Captive Portal Remediation] : クライアントによりキャプティブ ポータル（ホットスポット）が検出された場合、クローズ接続障害ポリシーにより適用されるネットワーク アクセスの制限が AnyConnect により解除されます。ホテルや空港では、ユーザが必ずブラウザを開いてインターネット アクセスの許可に必要な条件を満たすことができるようにするため、キャプティブ ポータルを使用するのが一般的です。デフォルトの場合、このパラメータはオフになっており、セキュリティは最高度に設定されます。ただし、クライアントから VPN へ接続する必要があるにもかかわらず、キャプティブ ポータルによりそれが制限されている場合は、このパラメータをオンにする必要があります。
  - [Remediation Timeout] : AnyConnect によりネットワーク アクセスの制限が解除されるまでの時間（分）。このパラメータは、[Allow Captive Portal Remediation] パラメータがオンになっており、かつクライアントによりキャプティブ ポータルが検出された場合に適用されます。キャプティブ ポータルの要件を満たすことができるだけの十分な時間を指定します（5 分など）。
  - [Apply Last VPN Local Resource Rules] : VPN が到達不能の場合、クライアントでは ASA から受信した最後のクライアント ファイアウォールが適用されます。この中には、ローカル LAN 上のリソースへのアクセスを許可する ACL が含まれている場合もあります。

[PPP Exclusion] : PPP 接続上で VPN トンネルについて、除外ルートを特定するかどうかや、除外ルートを特定する方法を指定します。これにより、クライアントでは、セキュリティ ゲートウェイよりも先を宛先としてトンネリングされたトラフィックから、このセキュリティ ゲートウェイを宛先とするトラフィックを除外することができます。除外ルートは、セキュアでないルートとして AnyConnect GUI の [Route Details] 画面に表示されます。この機能をユーザ設定可能にした場合、ユーザは PPP 除外設定の読み取りや変更を行うことができます。

- [Automatic] : PPP 除外を有効にします。AnyConnect では自動的に、PPP サーバの IP アドレスが使用されます。この値は、自動検出による IP アドレスの取得に失敗すした場合にのみ変更するよう、ユーザに指示してください。
- [Disabled] : PPP 除外は適用されません。
- [Override] : 同様に PPP 除外を有効にします。自動検出で PPP サーバの IP アドレスを取得できず、かつ PPP 除外をユーザ設定可能に設定している場合は、ユーザに対して「ユーザによる PPP 除外の上書き」（P.3-79）の説明に従うよう指示してください。

[PPP Exclusion Server IP]：PPP 除外に使用されるセキュリティ ゲートウェイの IP アドレス。

[Enable Scripting]：OnConnect スクリプトおよび OnDisconnect スクリプトがセキュリティ アプライアンスのフラッシュ メモリに存在する場合はそれらを起動します。

- [Terminate Script On Next Event]：スクリプト処理可能な別のイベントへの移行が発生した場合に、実行中のスクリプト プロセスを終了します。たとえば、VPN セッションが終了すると、AnyConnect では実行中の OnConnect スクリプトが終了し、クライアントで新しい VPN セッションが開始すると、実行中の OnDisconnect スクリプトが終了します。Microsoft Windows 上のクライアントでは OnConnect スクリプトまたは OnDisconnect スクリプトによって起動した任意のスクリプト、およびその従属スクリプトもすべて終了します。Mac OS および Linux 上のクライアントでは、OnConnect スクリプトまたは OnDisconnect スクリプトのみ終了し、子スクリプトは終了しません。
- [Enable Post SBL On Connect Script]：SBL で VPN セッションが確立された場合に OnConnect スクリプトが（存在すれば）起動されるようにします。（VPN エンドポイントで Microsoft Windows 7、Windows XP、または Windows Vista が実行されている場合にのみサポート）。

[Retain VPN On Logoff]：ユーザが Windows OS からログオフした場合に、VPN セッションを維持するかどうかを指定します。

- [User Enforcement]：別のユーザがログインした場合に VPN セッションを終了するかどうかを指定します。このパラメータが適用されるのは、[Retain VPN On Logoff] がオンになっており、かつ VPN セッションが確立されている間に元のユーザが Windows からログオフした場合のみです。

[Authentication Timeout Values]：デフォルトでは、AnyConnect は接続試行を終了するまでに、セキュア ゲートウェイからの認証を最大 12 秒間待ちます。その時間が経過すると、認証がタイムアウトになったことを示すメッセージが表示されます。10 ～ 120 の範囲で秒数を入力します。

このペインに表示されるクライアント機能に関するより詳細な設定情報については、次の各項を参照してください。

- 「ローカル プロキシ接続」（P.3-66）
- 「ブラウザのプロキシ設定を無視するためのクライアントの設定」（P.3-75）
- 「最適ゲートウェイ選択」（P.3-67）
- 「Trusted Network Detection の設定」（P.3-21）
- 「VPN 常時接続」（P.3-23）
- 「VPN 常時接続に関する接続障害ポリシー」（P.3-29）
- 「キャプティブ ポータル ホットスポットの検出と修復」（P.3-32）
- 「L2TP または PPTP を介した AnyConnect」（P.3-78）
- 「認証タイムアウト コントロール」（P.3-74）

AnyConnect プロファイル エディタの [Backup Servers]

ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定できます。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるサーバに対して接続が試行され、必要に応じてリストを下方向へ移動します。

[Host Address]：バックアップ サーバ リストに表示する IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

[Add]：バックアップ サーバ リストにホスト アドレスを追加します。

[Move Up]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストを下方向へ移動します。

[Move Down]：選択したバックアップ サーバをリストの下方向に移動します。

[Delete]：サーバ リストからバックアップ サーバを削除します。

バックアップ サーバの設定に関する詳細については、「バックアップ サーバ リストの設定」（P.3-65）を参照してください。

AnyConnect プロファイル エディタの [Certificate Matching]

このペインでは、クライアントによる自動証明書選択の詳細設定に使用できるさまざまな属性の定義を有効にします。

[Key Usage]：受け入れ可能なクライアント証明書を選択する場合は、次のような証明書キー属性を使用できます。

- Decipher_Only：データを復号化します。他のビットは設定されません（Key_Agreement は除く）。
- Encipher_Only：データを暗号化します。他のビットは設定されません（Key_Agreement は除く）。
- CRL_Sign：CRL の CA 署名を確認します。
- Key_Cert_Sign：証明書の CA 署名を確認します。
- Key_Agreement：キー共有。
- Data_Encipherment：Key_Encipherment 以外のデータを暗号化します。
- Key_Encipherment：キーを暗号化します。
- Non_Repudiation：一部の処理を誤って拒否しないように、Key_Cert_sign および CRL_Sign 以外のデジタル署名を確認します。
- Digital_Signature：Non_Repudiation、Key_Cert_Sign、および CRL_Sign 以外のデジタル署名を確認します。

[Extended Key Usage]：次のキーの拡張用途設定を使用します。OID は丸カッコ内に記載してあります。

- ServerAuth（1.3.6.1.5.5.7.3.1）
- ClientAuth（1.3.6.1.5.5.7.3.2）
- CodeSign（1.3.6.1.5.5.7.3.3）
- EmailProtect（1.3.6.1.5.5.7.3.4）
- IPSecEndSystem（1.3.6.1.5.5.7.3.5）
- IPSecTunnel（1.3.6.1.5.5.7.3.6）
- IPSecUser（1.3.6.1.5.5.7.3.7）
- TimeStamp（1.3.6.1.5.5.7.3.8）
- OCSPSign（1.3.6.1.5.5.7.3.9）
- DVCS（1.3.6.1.5.5.7.3.10）

[Custom Extended Match Key (Max 10)]：カスタム拡張照合キー（もしあれば）を指定します（最大 10 個）証明書は入力したすべての指定キーに一致する必要があります。OID 形式でキーを入力します（1.3.6.1.5.5.7.3.11 など）。

[Distinguished Name (Max 10)]：受け入れ可能なクライアント証明書を選択する際に完全一致基準として使用する識別名（DN）を指定します。

[Name]：照合に使用する識別名（DN）。

- CN：サブジェクトの一般名
- C：サブジェクトの国
- DC：ドメイン コンポーネント
- DNQ：サブジェクトの DN 修飾子
- EA：サブジェクトの電子メール アドレス
- GENQ：サブジェクトの GEN 修飾子
- GN：サブジェクトの名
- I：サブジェクトのイニシャル
- L：サブジェクトの都市
- N：サブジェクトの非構造体名
- O：サブジェクトの会社
- OU：サブジェクトの部署
- SN：サブジェクトの姓
- SP：サブジェクトの州
- ST：サブジェクトの州
- T：サブジェクトの敬称
- ISSUER-CN：発行元の一般名
- ISSUER-DC：発行元のコンポーネント
- ISSUER-SN：発行元の姓
- ISSUER-GN：発行元の名
- ISSUER-N：発行元の非構造体名
- ISSUER-I：発行元のイニシャル
- ISSUER-GENQ：発行元の GEN 修飾子
- ISSUER-DNQ：発行元の DN 修飾子
- ISSUER-C：発行元の国
- ISSUER-L：発行元の都市
- ISSUER-SP：発行元の州
- ISSUER-ST：発行元の州
- ISSUER-O：発行元の会社
- ISSUER-OU：発行元の部署
- ISSUER-T：発行元の敬称
- ISSUER-EA：発行元の電子メール アドレス

[Pattern]：照合する文字列を指定します。照合するパターンには、目的の文字列部分のみ含まれている必要があります。パターン照合構文や正規表現構文を入力する必要はありません。入力した場合、その構文は検索対象の文字列の一部と見なされます。

abc.cisco.com という文字列を例とした場合、cisco.com で照合するためには、入力するパターンを cisco.com とする必要があります。

[Wildcard]：[Enabled] を指定するとワイルドカード パターン照合が含まれます。ワイルドカードが有効であれば、パターンは文字列内のどの場所でも使用できます。

[Operator]：この DN で照合する場合に使用する演算子です。

- [Equal]：== と同等
- [Not Equal]：!= と同等

[Match Case]：大文字と小文字を区別したパターン照合を有効にする場合はオンにします。

証明書の照合に関するより詳細な設定情報については、「証明書照合の設定」（P.3-55）を参照してください。

AnyConnect プロファイル エディタの [Certificate Enrollment]

[Certificate Enrollment]：AnyConnect で、クライアント認証に使用する証明書のプロビジョニングおよび更新を行う場合に、Simple Certificate Enrollment Protocol（SCEP）を使用できるようにします。

[Certificate Expiration Threshold]：AnyConnect が、証明書の有効期限の何日前にユーザに対して証明書の失効が近づいていることを警告する日数（RADIUS パスワード管理ではサポートされません）。デフォルトは 0（警告は表示しない）です。値の範囲は 0 ～ 180 日です。

[Automatic SCEP Host]：SCEP 証明書取得が設定されている ASA のホスト名および接続プロファイル（トンネル グループ）を指定します。ASA の完全修飾ドメイン名（FQDN）または接続プロファイル名を入力してください （ホスト名 *asa.cisco.com*、接続プロファイル名 *scep_eng* など）。

[CA URL]：レガシー SCEP の場合、SCEP CA サーバを特定します。CA サーバの FQDN または IP アドレスを入力してください （*http://ca01.cisco.com* など）。

- [Prompt For Challenge PW]：有効にすると、証明書をユーザが手動で要求できるようになります。ユーザが [Get Certificate] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。
- [Thumbprint]：CA の証明書サムプリント。SHA1 ハッシュまたは MD5 ハッシュを使用します。

（注） CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行したサーバ証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

[Certificate Contents]：SCEP 登録要求に含める証明書の内容を指定します。

- Name (CN)：証明書での一般名。
- Department (OU)：証明書に指定されている部署名。
- Company (O)：証明書に指定されている会社名。
- State (ST)：証明書に指定されている州 ID。
- State (SP)：別の州 ID。
- Country (C)：証明書に指定されている国 ID。

- Email (EA)：電子メール アドレス。次の例では、[Email (EA)] は %USER%@cisco.com です。%USER% は、ユーザの ASA ユーザ名ログイン クレデンシャルに対応します。
- Domain (DC)：ドメイン コンポーネント。次の例では、[Domain (DC)] は cisco.com に設定されています。
- SurName (SN)：姓または名。
- GivenName (GN)：通常は名。
- UnstructName (N)：定義されていない名前。
- Initials (I)：ユーザのイニシャル。
- Qualifier (GEN)：ユーザの世代修飾子 （「Jr.」、「III.」など）。
- Qualifier (DN)：完全 DN の修飾子。
- City (L)：都市 ID。
- Title (T)：個人の敬称 （Ms.、Mrs.、Mr. など）。
- CA Domain：SCEP 登録に使用されます。通常は CA ドメイン。
- Key size：登録する証明書用に生成された RSA キーのサイズ。

[Display Get Certificate Button]：次の条件下で AnyConnect GUI が [Get Certificate] ボタンを表示できるようにします。

- 証明書は [Certificate Expiration Threshold] で定義された期間内に期限が切れるよう設定されている（RADIUS ではサポートされません）。
- 証明書の期限が切れている。
- 証明書がない。
- 証明書を照合できない。

[Certificate Enrollment] に関するより詳細な設定情報については、「SCEP による認証登録の設定」（P.3-45）を参照してください。

AnyConnect プロファイル エディタの [Mobile Policy]

このペインでは、Windows Mobile 上で実行中の AnyConnect で使用するパラメータを設定します。

- [Device Lock Required]：VPN 接続を確立する前に Windows Mobile デバイスに対してパスワードまたは PIN を設定する必要があります。これが適用されるのは、Microsoft Local Authentication Plug-ins（LAPs）を使用する Windows Mobile デバイスのみです。
- [Maximum Timeout Minutes]：デバイス ロックが有効になるまでの最長時間（単位は分）。設定は必須です。
- [Minimum Password Length]：デバイス ロック用のパスワードまたは PIN に必要な最低文字数を指定します。
- [Password Complexity]：必要なデバイス ロックのパスワードに対して複雑度を指定します。
  - [alpha]：英数字のパスワードであることが必要。
  - [pin]：数字の PIN であることが必要。
  - [strong]：7 文字以上で構成され、うち最低 3 文字は大文字、小文字、数字、句読記号のいずれかである強度の高い英数字のパスワードであることが必要。

AnyConnect プロファイル エディタの [Server List]

クライアント GUI に表示されるサーバ リストの設定を行うことができます。ユーザは、VPN 接続を確立する際、このリストでサーバを選択することができます。

[Server List] テーブルの列は次のとおりです。

- [Hostname]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアス。
- [Host Address]：サーバの IP アドレスまたは FQDN。
- [User Group]：[Host Address] と組み合わせて使用することによりグループ ベースの URL が構成されます。
- [Automatic SCEP Host]：クライアント認証に使用する証明書のプロビジョニング用および更新用として指定された Simple Certificate Enrollment Protocol。
- [CA URL]：このサーバが認証局（CA）へ接続する際に使用する URL。

[Add/Edit]：サーバのパラメータを指定できる [Server List Entry] ダイアログを起動します。

[Delete]：サーバ リストからサーバを削除します。

[Details]：サーバのバックアップ サーバまたは CA URL に関する詳細情報を表示します。

AnyConnect プロファイル エディタの [Add/Edit Server List]

このペインでは、サーバとそのバックアップ サーバ、およびロード バランシング バックアップ デバイスを追加します。

[Hostname]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアスを入力します。

[Host Address]：サーバの IP アドレスまたは FQDN を指定します。

（注）

- [Host Address] フィールドに IP アドレスまたは FQDN を指定すると、[Host Name] フィールドのエントリが AnyConnect Client トレイ フライアウト内の接続ドロップダウン リストに表示されるサーバのラベルになります。
- [Hostname] フィールドで FQDN のみを指定し、[Host Address] フィールドでは IP アドレスを指定しない場合、[Hostname] フィールドの FQDN が DNS で解決されます。
- IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイの使用はサポートしていません。

[User Group]：ユーザ グループを指定します。このユーザ グループとホスト アドレスを組み合わせてグループ ベースの URL が構成されます。

（注） プライマリ プロトコルを IPsec として指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。

[Backup Server List]：ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定できます。サーバで障害が発生した場合、クライアントではまずリストの先頭にあるサーバに対して接続が試行され、必要に応じてリストを下方向へ移動します。

- [Host Address]：バックアップ サーバ リストに表示する IP アドレスまたは FQDN を指定します。クライアントでは、ホストに接続できない場合には、バックアップ サーバへの接続が試行されます。
- [Add]：バックアップ サーバ リストにホスト アドレスを追加します。
- [Move Up]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストを下方向へ移動します。
- [Move Down]：選択したバックアップ サーバをリストの下方向に移動します。
- [Delete]：サーバ リストからバックアップ サーバを削除します。

[Load Balancing Server List]：このサーバ リスト エントリのホストがセキュリティ アプライアンスのロード バランシング クラスタであり、かつ常時接続機能が有効になっている場合は、このリストでクラスタのバックアップ デバイスを指定します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスは常時接続機能によりブロックされます。

- [Host Address]：ロードバランシング クラスタにあるバックアップサーバの IP アドレスまたは FQDN を指定します。
- [Add]：ロード バランシング バックアップ サーバ リストにアドレスを追加します。
- [Delete]：ロード バランシング バックアップ サーバをリストから削除します。

[Primary Protocol]：この ASA も接続するプロトコル（SSL または IKEv2 を使用した IPsec）を指定します。デフォルトは SSL です。

[Standard Authentication Only]：デフォルトでは、AnyConnect クライアントは独自の AnyConnect EAP 認証方式を使用します。クライアントで標準ベースの方式を使用する場合は、これをオンにして設定します。ただし、そうした場合はクライアントのダイナミック ダウンロード機能が制限され、一部の機能が無効になります。

（注） 認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、ASA でセッション タイムアウト、アイドル タイムアウト、接続解除タイムアウト、スプリット トンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

[IKE Identity]：標準ベースの EAP 認証方式を選択した場合、このフィールドにグループまたはドメインをクライアント アイデンティティとして入力できます。クライアントは、文字列を ID_GROUP タイプ IDi ペイロードとして送信します。デフォルトでは、文字列は *$AnyConnectClient$* です。

[CA URL]：SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します（*http://ca01.cisco.com* など）。

- [Prompt For Challenge PW]：有効にすると、証明書をユーザが手動で要求できるようになります。ユーザが [Get Certificate] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。
- [Thumbprint]：CA の証明書サムプリント。SHA1 ハッシュまたは MD5 ハッシュを使用します。

（注）　CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行した証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

サーバ リストの作成に関するより詳細な設定情報については、「サーバ リストの設定」（P.3-60）を参照してください。