Cisco ASA シリーズ VPN ASDM コンフィギュレーション ガイド

ソフトウェア バージョン 7.3
ASA 5506-X、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X、ASA サービス モジュール、適応型セキュリティ仮想アプライアンス向け

リリース日：2014 年 7 月 24 日
更新日：2014 年 12 月 18 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。住所、電話番号、FAX 番号は 以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices

Text Part Number: なし、オンライン専用

Cisco ASA シリーズ VPN ASDM コンフィギュレーション ガイド

このマニュアルについて

マニュアルの目的

このマニュアルの目的は、ASDM を使用して適応型セキュリティ アプライアンス（ASA）上で VPN を設定する支援をすることです。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

このマニュアルは、Cisco ASA シリーズに適用されます。このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

（注） ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。同様に、古いメジャー バージョンまたはマイナー バージョンのメンテナンス リリースに機能が追加された場合、この新機能は、以降のすべての ASA リリースで使用できない場合でも、ASDM のマニュアルに含まれています。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。各 ASA のバージョンでサポートされている ASDM の最小バージョンについては、『Cisco ASA Series Compatibility』を参照してください。

関連資料

詳細については、「*Navigating the Cisco ASA Series Documentation*」（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
太字の `courier` フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字の `courier` フォント**で示しています。
イタリック体の `courier` フォント	ユーザが値を指定する引数は、***イタリック体の `courier` フォント***で示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

PART 1

サイト間 VPN およびクライアント VPN

VPN ウィザード

リリース日：2014 年 7 月 24 日
更新日：2014 年 12 月 18 日

VPN の概要

ASA は、ユーザがプライベートな接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することにより、バーチャル プライベート ネットワークを構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。

LAN-to-LAN 接続で IPv4 と IPv6 の両方のアドレッシングが使用されているときに、ASA で VPN トンネルがサポートされるのは、両方のピアが ASA であり、かつ両方の内部ネットワークのアドレッシング方式が一致している（両方とも IPv4 または IPv6）場合です。これは、両方のピアの内部ネットワークが IPv6 で外部ネットワークが IPv6 の場合にも当てはまります。

セキュアな接続はトンネルと呼ばれ、ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向のトンネル エンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方の側に送信することができます。そのエンドポイントで、パケットはカプセル化が解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

VPN ウィザードでは、基本的な LAN-to-LAN およびリモート アクセス VPN 接続を設定して、認証のための事前共有キーまたはデジタル証明書を割り当てることができます。ASDM を使用して拡張機能を編集および設定してください。

ここでは、次の 4 つの VPN ウィザードについて説明します。

- 「Clientless SSL VPN Wizard」（P.1-2）

  ASA クライアントレス SSL VPN では、ほぼすべてのインターネット接続環境からの Secure Socket Layer（SSL）リモート アクセス接続機能を提供します。Web ブラウザとそのネイティブの SSL 暗号化機能だけでアクセスが可能です。このブラウザベースの VPN により、適応型セキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを確立できます。認証されると、ユーザにはポータル ページが表示され、サポートされる特定の内部リソースにアクセスできるようになります。ネットワーク管理者は、グループ単位でユーザにリソースへのアクセス権限を付与します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

- 「AnyConnect VPN Wizard」（P.1-3）

  Cisco AnyConnect VPN クライアントは ASA へのセキュアな SSL 接続または IPsec（IKEv2）接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN トンネリングが可能となります。事前にクライアントがインストールされていない場合、リモート ユーザは、クライアントレス VPN 接続を受け入れるように設定されたインターフェイスの IP アドレスをブラウザに入力します。ASA は、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロードが完了すると、クライアントが自動的にインストールおよび設定され、セキュア接続が確立されます。接続終了時にクライアントが残されるか、アンインストールされるかは、ASA の設定で決まります。事前にクライアントがインストールされている場合は、ユーザの認証時に、ASA がクライアントのリビジョンを検査し、必要に応じてクライアントをアップグレードします。

- 「IPsec IKEv2 Remote Access Wizard」（P.1-5）

  IKEv2 によって、他のベンダーの VPN クライアントが ASA に接続できます。このサポートによってセキュリティが強化されるとともに、IPsec リモート アクセスに関して国や地方自治体が定める要件も満たされます。

- 「IPsec IKEv1 Remote Access Wizard」（P.1-7）
- 「IPsec Site-to-Site VPN Wizard」（P.1-12）

Clientless SSL VPN Wizard

このウィザードでは、サポートされる特定の内部リソースに対する、ポータル ページからのクライアントレス ブラウザベース接続をイネーブルにします。

[SSL VPN Interface]

接続プロファイルと、SSL VPN ユーザの接続先となるインターフェイスを指定します。

- [Connection Profile Name]：接続プロファイルの名前を指定します。
- [SSL VPN Interface]：SSL VPN 接続のためにユーザがアクセスするインターフェイスです。
- [Digital Certificate]：ASA の認証のために ASA からリモート Web ブラウザに何を送信するかを指定します。
  - [Certificate]：ドロップダウン リストから選択します。
- [Accessing the Connection Profile]
  - [Connection Group Alias/URL]：グループ エイリアスはログイン時に [Group] ドロップダウン リストから選択されます。この URL が Web ブラウザに入力されます。
  - [Display Group Alias list at the login page]：ログイン ページにグループ エイリアスのリストを表示する場合にオンにします。

[User Authentication]

このペインでは、認証情報を指定します。

- [Authenticate using a AAA server group]：ASA がリモート AAA サーバ グループにアクセスしてユーザを認証できるようにする場合にイネーブルにします。
  - [AAA Server Group Name]：事前設定されたグループのリストから AAA サーバ グループを選択するか、[New] をクリックして新しいグループを作成します。

- [Authenticate using the local user database]：ASA に保存されているローカル データベースに新しいユーザを追加します。
  - [Username]：ユーザのユーザ名を作成します。
  - [Password]：ユーザのパスワードを作成します。
  - [Confirm Password]：確認のために同じパスワードを再入力します。
  - [Add/Delete]：ローカル データベースにユーザを追加またはデータベースから削除します。

[Group Policy]

グループ ポリシーによって、ユーザ グループの共通属性を設定します。新しいグループ ポリシーを作成するか、または既存のポリシーを選択して修正します。

- [Create new group policy]：新しいグループ ポリシーを作成できます。新しいポリシーの名前を入力します。
- [Modify existing group policy]：修正する既存のグループ ポリシーを選択します。

[Bookmark List]

グループ イントラネット Web サイトのリストを設定します。これらのサイトは、ポータル ページにリンクとして表示されます。例としては、https://intranet.acme.com、rdp://10.120.1.2、vnc://100.1.1.1 などがあります。

- [Bookmark List]：ドロップダウン リストから選択します。
- [Manage]：[Configure GUI Customization Object] ダイアログボックスを開く場合にクリックします。

AnyConnect VPN Wizard

このウィザードは、AnyConnect VPN クライアントからの VPN 接続を受け入れるように ASA を設定するときに使用します。このウィザードでは、フル ネットワーク アクセスができるように IPsec（IKEv2）プロトコルまたは SSL VPN プロトコルを設定します。VPN 接続が確立したときに、ASA によって自動的に AnyConnect VPN クライアントがエンド ユーザのデバイスにアップロードされます。

このウィザードを実行しても、事前展開シナリオにおいて自動的に IKEv2 プロファイルが適用されるわけではないことについてユーザに注意を促します。IKEv2 を正常に事前展開するのに必要な指示または手順を示す必要があります。

[Connection Profile Identification]

[Connection Profile Identification] では、リモート アクセス ユーザに対する ASA を指定します。

- [Connection Profile Name]：リモート アクセス ユーザが VPN 接続のためにアクセスする名前を指定します。
- [VPN Access Interface]：リモート アクセス ユーザが VPN 接続のためにアクセスするインターフェイスを選択します。

[VPN Protocols]

この接続プロファイルに対して許可する VPN プロトコルを指定します。

AnyConnect クライアントのデフォルトは SSL です。接続プロファイルの VPN トンネル プロトコルとして IPsec をイネーブルにした場合は、IPsec をイネーブルにしたクライアント プロファイルを作成して展開することも必要になります（作成するには、ASDM のプロファイル エディタを使用します）。

AnyConnect クライアントの WebLaunch の代わりに事前展開する場合は、最初のクライアント接続で SSL を使用し、クライアント プロファイルをセッション中に ASA から受け取ります。以降の接続では、クライアントはそのプロファイルで指定されたプロトコル（SSL または IPsec）を使用します。IPsec が指定されたプロファイルをクライアントとともに事前展開した場合は、最初のクライアント接続で IPsec が使用されます。IPsec をイネーブルにした状態のクライアント プロファイルを事前展開する方法の詳細については、『*AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。

- SSL
- IPsec (IKE v2)
- [Device Certificate]：リモート アクセス クライアントに対する ASA を指定します。AnyConnect の機能の中には、Always on や IPsec/IKEv2 のように、有効なデバイス証明書が ASA に存在することを要件とするものがあります。
- [Manage]：[Manage] を選択すると [Manage Identity Certificates] ウィンドウが開きます。
  - [Add]：ID 証明書とその詳細情報を追加するには、[Add] を選択します。
  - [Show Details]：特定の証明書を選択して [Show Details] をクリックすると、[Certificate Details] ウィンドウが開き、その証明書の発行対象者と発行者が表示されるほか、シリアル番号、使用方法、対応するトラストポイント、有効期間などが表示されます。
  - [Delete]：削除する証明書を強調表示して [Delete] をクリックします。
  - [Export]：証明書を強調表示して [Export] をクリックすると、その証明書をファイルにエクスポートできます。このときに、暗号化パスフレーズを付けるかどうかを指定できます。
  - [Enroll ASA SSL VPN with Entrust]：Entrust からの SSL Advantage デジタル証明書を使用すると、すぐに Cisco ASA SSL VPN アプライアンスの稼働を開始できます。

[Client Images]

ASA は、クライアント デバイスがエンタープライズ ネットワークにアクセスするときに、最新の AnyConnect パッケージをそのデバイスに自動的にアップロードすることができます。ブラウザのユーザ エージェントとイメージとの対応を、正規表現を使用して指定できます。また、接続の設定に要する時間を最小限にするために、最もよく使用されるオペレーティング システムをリストの先頭に移動できます。

[Authentication Methods]

この画面では、認証情報を指定します。

- [AAA server group]：ASA がリモート AAA サーバ グループにアクセスしてユーザを認証できるようにする場合にイネーブルにします。AAA サーバ グループを、事前設定されたグループのリストから選択するか、[New] をクリックして新しいグループを作成します。
- [Local User Database Details]：ASA 上に格納されているローカル データベースに新しいユーザを追加します。
  - [Username]：ユーザのユーザ名を作成します。
  - [Password]：ユーザのパスワードを作成します。
  - [Confirm Password]：確認のために同じパスワードを再入力します。
  - [Add/Delete]：ローカル データベースにユーザを追加またはデータベースから削除します。

[Client Address Assignment]

リモート AnyConnect ユーザのための IP アドレス範囲を指定します。

- [IPv4 Address Pools] : SSL VPN クライアントは、ASA に接続したときに新しい IP アドレスを受け取り ます。クライアントレス接続では新しい IP アドレスは不要です。アドレス プールでは、リモート クライアントが受け取ることのできるアドレス範囲が定義されます。既存の IP アドレス プールを選択するか、[New] をクリックして新しいプールを作成します。

  [New] を選択した場合は、開始と終了の IP アドレスおよびサブネット マスクを指定する必要があります。

- [IPv6 Address Pool] : 既存の IP アドレス プールを選択するか、[New] をクリックして新しいプールを作成します。

（注）　IPv6 アドレス プールは、IKEv2 接続プロファイル用には作成できません。

[Network Name Resolution Servers]

リモート ユーザが内部ネットワークにアクセスするときにどのドメイン名を解決するかを指定します。

- [DNS Servers]：DNS サーバの IP アドレスを入力します。
- [WINS Servers]：WINS サーバの IP アドレスを入力します。
- [Domain Name]：デフォルトのドメイン名を入力します。

[NAT Exempt]

ASA 上でネットワーク変換がイネーブルに設定されている場合は、VPN トラフィックに対してこの変換を免除する必要があります。

[AnyConnect Client Deployment]

次の 2 つの方法のいずれかを使用して、AnyConnect クライアント プログラムをクライアント デバイスにインストールできます。

- WebLaunch：AnyConnect クライアント パッケージは、Web ブラウザを使用して ASA にアクセスしたときに自動的にインストールされます。
- 事前展開：手動で AnyConnect クライアント パッケージをインストールします。

[Allow Web Launch] は、すべての接続に影響が及ぶグローバル設定です。このチェックボックスがオフ（許可しない）の場合は、AnyConnect SSL 接続とクライアントレス SSL 接続は機能しません。

事前展開の場合は、disk0:/test2_client_profile.xml プロファイル バンドルの中に .msi ファイルがあり、このクライアント プロファイルを ASA から AnyConnect パッケージに入れておく必要があります。これは、IPsec 接続を期待したとおりに確実に動作させるためです。

IPsec IKEv2 Remote Access Wizard

IKEv2 Remote Access Wizard を使用して、モバイル ユーザなどの VPN クライアントの安全なリモート アクセスを設定し、リモート IPsec ピアに接続するインターフェイスを指定します。

[Connection Profile Identification]

[Connection Profile Name] に接続プロファイルの名前を入力し、[VPN Access Interface] で IPsec IKEv2 リモート アクセスに使用する VPN アクセス インターフェイスを選択します。

- [Connection Profile Name]：名前を入力して、この IPsec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウンティング サーバ、デフォルト グループ ポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定する接続ポリシーでは、認証方式を指定し、ASA のデフォルトのグループ ポリシーを使用します。
- [VPN Access Interface]：リモート IPsec ピアとのセキュアなトンネルを確立するインターフェイスを選択します。ASA に複数のインターフェイスがある場合は、このウィザードを実行する前に VPN コンフィギュレーションを計画し、セキュアな接続を確立する予定のリモート IPsec ピアごとに、使用するインターフェイスを特定しておく必要があります。

[Authentication] ページ

[IKE Peer Authentication]：リモート サイト ピアは、事前共有キー、証明書、または EAP を使用したピア認証のいずれかを使用して認証します。

- [Pre-shared Key]：1 ～ 128 文字の英数字文字列を入力します。

  事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

  IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモート サイトの管理者と事前共有キーを交換してください。
- [Enable Certificate Authentication]：オンにすると、認証に証明書を使用できます。
- [Enable peer authentication using EAP]：オンにすると、認証に EAP を使用できます。このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。
- [Send an EAP identity request to the client]：リモート アクセス VPN クライアントに EAP 認証要求を送信できます。

[IKE Local Authentication]

- ローカル認証をイネーブルにし、事前共有キーまたは証明書のいずれかを選択します。
  - [Preshared Key]：1 ～ 128 文字の英数字文字列を入力します。
  - [Certificate]：ローカル ASA とリモート IPsec ピアの間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、あらかじめ CA への登録を済ませ、1 つ以上の証明書を ASA にダウンロードしておく必要があります。

    デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

    デジタル証明書を使用するには、デジタル証明書を発行する認証局（CA）に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

    2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

[Authentication Methods]

IPsec IKEv2 リモート アクセスでは RADIUS 認証のみがサポートされています。

- [AAA Server Group]：先に構成された AAA サーバ グループを選択します。
- [New]：新しい AAA サーバ グループを設定する場合にクリックします。
- [AAA Server Group Details]：この領域を使用して、AAA サーバ グループを必要に応じて変更します。

[Client Address Assignment]

画面上にすでに表示されている内容が最も役立ちます。

IPv4 および IPv6 のアドレス プールを作成するか、選択します。リモート アクセス クライアントには、IPv4 または IPv6 のプールのアドレスが割り当てられます。両方を設定した場合は、IPv4 アドレスが優先されます。詳細については、「*ローカル IP アドレス プールの設定*」を参照してください。

[Network Name Resolution Servers]

リモート ユーザが内部ネットワークにアクセスするときにどのようにドメイン名を解決するかを指定します。

- [DNS Servers]：DNS サーバの IP アドレスを入力します。
- [WINS Servers]：WINS サーバの IP アドレスを入力します。
- [Default Domain Name]：デフォルトのドメイン名を入力します。

[NAT Exempt]

- [Exempt VPN traffic from Network Address Translation]：ASA で NAT がイネーブルになっている場合は、このチェックボックスをオンにする必要があります。

IPsec IKEv1 Remote Access Wizard

（注） Cisco VPN Client は耐用年数末期で、サポートが終了しています。AnyConnect セキュア モビリティ クライアントにアップグレードする必要があります。

IKEv1 Remote Access Wizard を使用して、モバイル ユーザなどの VPN クライアントの安全なリモート アクセスを設定し、リモート IPsec ピアに接続するインターフェイスを指定します。

- [VPN Tunnel Interface]：リモート アクセス クライアントで使用するインターフェイスを選択します。ASA に複数のインターフェイスがある場合は、このウィザードを実行する前に ASA でインターフェイスを設定します。
- [Enable inbound IPsec sessions to bypass interface access lists]：ASA によって常に許可される（つまり、インターフェイスの access-list 文をチェックしない）ように、IPsec 認証の着信セッションをイネーブルにします。着信セッションがバイパスするのは、インターフェイス ACL だけです。設定されたグループ ポリシー、ユーザ、およびダウンロードされた ACL は適用されます。

[Remote Access Client]

さまざまなタイプのリモート アクセス ユーザが、この ASA への VPN トンネルを開くことができます。このトンネルの VPN クライアントのタイプを選択します。

- [VPN Client Type]
  - [Easy VPN Remote product]
  - [Microsoft Windows client using L2TP over IPsec]：PPP 認証プロトコルを指定します。選択肢は、PAP、CHAP、MS-CHAP-V1、MS-CHAP-V2、および EAP-PROXY です。

    [PAP]：認証中にクリアテキストのユーザ名とパスワードを渡すので、安全ではありません。

    [CHAP]：サーバのチャレンジに対する応答で、クライアントは暗号化されたチャレンジとパスワードおよびクリアテキストのユーザ名を返します。このプロトコルは、PAP より安全ですが、データは暗号化されません。

    [MS-CHAP, Version 1]：CHAP と似ていますが、サーバは、CHAP のようなクリアテキストのパスワードではなく、暗号化したパスワードだけを保存および比較するので安全です。

    [MS-CHAP, Version 2]：MS-CHAP, Version 1 以上のセキュリティ強化機能が含まれています。

    [EAP-Proxy]：EAP をイネーブルにします。これによって ASA は、PPP の認証プロセスを外部の RADIUS 認証サーバに代行させます。

    リモート クライアントでプロトコルが指定されていない場合は、指定しないでください。
  - 指定するのは、クライアントからトンネル グループ名が username@tunnelgroup として送信される場合です。

VPN クライアント認証方式とトンネル グループ名

認証方式を設定し、接続ポリシー（トンネル グループ）を作成するには、[VPN Client Authentication Method and Name] ペインを使用します。

- [Authentication Method]：リモート サイト ピアは、事前共有キーか証明書のいずれかを使用して認証します。
  - [Pre-shared Key]：ローカル ASA とリモート IPsec ピアの間の認証で事前共有キーを使用する場合にクリックします。

    事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

    IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモート サイトの管理者と事前共有キーを交換してください。
  - [Pre-shared Key]：1 ～ 128 文字の英数字文字列を入力します。
  - [Certificate]：ローカル ASA とリモート IPsec ピアの間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、あらかじめ CA への登録を済ませ、1 つ以上の証明書を ASA にダウンロードしておく必要があります。

    デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

    デジタル証明書を使用するには、デジタル証明書を発行する認証局（CA）に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

[Certificate Signing Algorithm]：デジタル証明書署名アルゴリズムを表示します（RSA の場合は rsa-sig）。

  - [Challenge/response authentication (CRACK)]：クライアントが RADIUS などの一般的な方式を使用して認証を行い、サーバが公開キーによる認証方式を使用している場合に、強力な相互認証を実現します。セキュリティ アプライアンスは、Nokia 92xx Communicator Series デバイスで Nokia VPN Client を認証するために、IKE オプションとして CRACK をサポートしています。

- [Tunnel Group Name]：名前を入力して、この IPsec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウンティング サーバ、デフォルト グループ ポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定する接続ポリシーでは、認証方式を指定し、ASA のデフォルトのグループ ポリシーを使用します。

[Client Authentication]

[Client Authentication] ペインでは、ASA がリモート ユーザを認証するときに使用する方法を選択します。次のオプションのいずれかを選択します。

- [Authenticate using the local user database]：ASA の内部の認証方式を使用する場合にクリックします。この方式は、ユーザの数が少なくて安定している環境で使用します。次のペインでは、ASA に個々のユーザのアカウントを作成できます。
- [Authenticate using an AAA server group]: リモート ユーザ認証で外部サーバ グループを使用する場合にクリックします。
  - [AAA Server Group Name]：先に構成された AAA サーバ グループを選択します。
  - [New...]：新しい AAA サーバ グループを設定する場合にクリックします。

[User Accounts]

[User Accounts] ペインでは、認証を目的として、ASA の内部ユーザ データベースに新しいユーザを追加します。

[Address Pool]

[Address Pool] ペインでは、ASA がリモート VPN クライアントに割り当てるローカル IP アドレスのプールを設定します。

- [Tunnel Group Name]：このアドレス プールが適用される接続プロファイル（トンネル グループ）の名前が表示されます。この名前は、[VPN Client Name and Authentication Method] ペイン（ステップ 3）で設定したものです。
- [Pool Name]：アドレス プールの記述 ID を選択します。
- [New...]：新しいアドレス プールを設定します。
- [Range Start Address]：アドレス プールの開始 IP アドレスを入力します。
- [Range End Address]：アドレス プールの終了 IP アドレスを入力します。
- [Subnet Mask]：（オプション）これらの IP アドレスのサブネット マスクを選択します。

[Attributes Pushed to Client (Optional)]

[Attributes Pushed to Client (Optional)] ペインでは、DNS サーバと WINS サーバおよびデフォルト ドメイン名についての情報をリモート アクセス クライアントに渡す動作を ASA に実行させます。

- [Tunnel Group]：アドレス プールが適用される接続ポリシーの名前を表示します。この名前は、[VPN Client Name and Authentication Method] ペインで設定したものです。
- [Primary DNS Server]：プライマリ DNS サーバの IP アドレスを入力します。
- [Secondary DNS Server]：セカンダリ DNS サーバの IP アドレスを入力します。
- [Primary WINS Server]：プライマリ WINS サーバの IP アドレスを入力します。
- [Secondary WINS Server]：セカンダリ WINS サーバの IP アドレスを入力します。
- [Default Domain Name]：デフォルトのドメイン名を入力します。

[IKE Policy]

Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれる IKE は、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。各 IKE ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。フェーズ 1 は、以後の IKE ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 では、データを保護するトンネルが作成されます。

[IKE Policy] ペインでは、フェーズ 1 IKE ネゴシエーションの条件を設定します。この条件には、データを保護し、プライバシーを守る暗号化方式、ピアの ID を確認する認証方式、および暗号キー判別アルゴリズムを強化する Diffie-Hellman グループが含まれます。このアルゴリズムを使用して、ASA は暗号キーとハッシュ キーを導出します。

- [Encryption]：フェーズ 2 ネゴシエーションを保護するフェーズ 1 SA を確立するために ASA が使用する、対称暗号化アルゴリズムを選択します。ASA は、次の暗号化アルゴリズムをサポートします。

アルゴリズム	説明
DES	データ暗号規格。56 ビット キーを使用します。
3DES	Triple DES。56 ビット キーを使用して暗号化を 3 回実行します。
AES-128	高度暗号化規格。128 ビット キーを使用します。
AES-192	192 ビット キーを使用する AES。
AES-256	256 ビット キーを使用する AES。

  デフォルトの 3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。同様に、AES オプションによるセキュリティは強力ですが、必要な処理量も増大します。

- [Authentication]：認証やデータ整合性の確保のために使用するハッシュ アルゴリズムを選択します。デフォルトは SHA です。MD5 のダイジェストは小さく、SHA よりもわずかに速いとされています。MD5 は、（きわめて困難ですが）攻撃により破れることが実証されています。ただし、ASA で使用される Keyed-Hash Message Authentication Code（HMAC）バージョンはこの攻撃を防ぎます。
- [Diffie-Hellman Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトの Group 2（1024 ビット Diffie-Hellman）は、Group 5（1536 ビット）と比較して、CPU の実行時間は短いですが、安全性は低くなります。

（注）　VPN 3000 シリーズ コンセントレータのデフォルト値は MD5 です。ASA と VPN コンセントレータの間の接続では、接続の両方の側で、フェーズ 1 と 2 の IKE ネゴシエーションの認証方式を同じにする必要があります。

[IPsec Settings (Optional)]

[IPsec Settings (Optional)] ペインでは、アドレス変換が不要なローカル ホスト/ネットワークを指定します。デフォルトにより ASA は、ダイナミックまたはスタティックのネットワーク アドレス変換（NAT）を使用して、内部ホストおよびネットワークの本当の IP アドレスを外部ホストから隠します。NAT は、信頼できない外部ホストによる攻撃の危険性を最小限に抑えますが、VPN によって認証および保護されているホストに対しては不適切な場合があります。

たとえば、ダイナミック NAT を使用する内部ホストは、プールから無作為に選択したアドレスと照合することにより、その IP アドレスを変換させます。外部ホストからは、変換されたアドレスだけが見えるようになります。本当の IP アドレスにデータを送信することによってこれらの内部ホストに到達しようとするリモート VPN クライアントは、NAT 免除ルールを設定しない限り、これらのホストには接続できません。

（注）　すべてのホストとネットワークを NAT から免除する場合は、このペインでは何も設定しません。エントリが 1 つでも存在すると、他のすべてのホストとネットワークは NAT に従います。

- [Interface]：選択したホストまたはネットワークに接続するインターフェイスの名前を選択します。
- [Exempt Networks]：選択したインターフェイス ネットワークから免除するホストまたはネットワークの IP アドレスを選択します。
- [Enable split tunneling]：リモート アクセス クライアントからのパブリック インターネット宛のトラフィックを暗号化せずに送信する場合に選択します。スプリット トンネリングにより、保護されたネットワークのトラフィックが暗号化され、保護されていないネットワークのトラフィックは暗号化されません。スプリット トンネリングをイネーブルにすると、ASA は、認証後に IP アドレスのリストをリモート VPN クライアントにプッシュします。リモート VPN クライアントは、ASA の背後にある IP アドレスへのトラフィックを暗号化します。他のすべてのトラフィックは、暗号化なしでインターネットに直接送り出され、ASA は関与しません。
- [Enable Perfect Forwarding Secrecy (PFS)]：フェーズ 2 IPsec キーを生成するときに Perfect Forward Secrecy を使用するかどうか、および使用する値のサイズを指定します。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPsec ネゴシエーションでは、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成に Diffie-Hellman 方式が採用されています。

  PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

  PFS は、接続の両側でイネーブルにする必要があります。

  - [Diffie-Hellman Group] : Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトの Group 2（1024 ビット Diffie-Hellman）は、Group 5（1536 ビット）と比較して、CPU の実行時間は短いですが、安全性は低くなります。

[Summary]

設定に問題なければ、[Finish] をクリックします。ASDM によって LAN-to-LAN のコンフィギュレーションが保存されます。[Finish] をクリックした後は、この VPN ウィザードを使用してこのコンフィギュレーションを変更することはできません。ASDM を使用して拡張機能を編集および設定してください。

IPsec Site-to-Site VPN Wizard

2 台の ASA デバイス間のトンネルを「サイトツーサイト トンネル」と呼び、これは双方向です。サイトツーサイト VPN トンネルでは、IPsec プロトコルを使用してデータが保護されます。

[Peer Device Identification]

- [Peer IP Address]：他のサイト（ピア デバイス）の IP アドレスを設定します。
- [VPN Access Interface]：サイトツーサイト トンネルに使用するインターフェイスを選択します。

[Traffic to Protects]

このステップでは、ローカル ネットワークおよびリモート ネットワークを指定します。これらのネットワークでは、IPsec 暗号化を使用してトラフィックが保護されます。

- [Local Networks]：IPsec トンネルで使用されるホストを指定します。
- [Remote Networks]：IPsec トンネルで使用されるネットワークを指定します。

[Security]

このステップでは、ピア デバイスとの認証の方法を設定します。単純な設定を選択するか、事前共有キーを指定できます。またさらに詳細なオプションについては、以下に説明する [Customized Configuration] を選択できます。

- [IKE Version]：どちらのバージョンを使用するかに応じて、[IKEv1] または [IKEv2] チェックボックスをオンにします。
- IKE version 1 Authentication Methods
  - [Pre-shared Key]：事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

    IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモート サイトの管理者と事前共有キーを交換してください。
  - [Device Certificate]：ローカル ASA とリモート IPsec ピアの間の認証で証明書を使用する場合にクリックします。

    デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

    2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。
- IKE version 2 Authentication Methods
  - [Local Pre-shared Key]：IPsec IKEv2 認証方式と暗号化アルゴリズムを指定します。
  - [Local Device Certificate]：VPN アクセスの認証を、セキュリティ アプライアンスを通して行います。
  - [Remote Peer Pre-shared Key]：ローカル ASA とリモート IPsec ピアの間の認証で事前共有キーを使用する場合にクリックします。
  - [Remote Peer Certificate Authentication]：このチェックボックスがオンのときは、ピア デバイスが証明書を使用してこのデバイスに対して自身の認証を行うことができます。

- [Encryption Algorithms]：このタブでは、データの保護に使用する暗号化アルゴリズムのタイプを選択します。
  - [IKE Policy]：IKEv1/IKEv2 認証方式を指定します。
  - [IPsec Proposal]：IPsec 暗号化アルゴリズムを指定します。
- [Perfect Forward Secrecy]
  - [Enable Perfect Forwarding Secrecy (PFS)]：フェーズ 2 IPsec キーを生成するときに Perfect Forward Secrecy を使用するかどうか、および使用する値のサイズを指定します。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPsec ネゴシエーションでは、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成に Diffie-Hellman 方式が採用されています。

    PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

    PFS は、接続の両側でイネーブルにする必要があります。
  - [Diffie-Hellman Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトの Group 2（1024 ビット Diffie-Hellman）は、Group 5（1536 ビット）と比較して、CPU の実行時間は短いですが、安全性は低くなります。

[NAT Exempt]

- [Exempt ASA side host/network from address translation]：ドロップダウン リストを使用して、アドレス変換から除外するホストまたはネットワークを選択します。

CHAPTER 2

IKE、ロード バランシング、および NAC

IKE は ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。バーチャル プライベート ネットワークの ASA を設定するには、システム全体に適用するグローバル IKE パラメータを設定します。また、VPN 接続を確立するためにピアがネゴシエートする IKE ポリシーも作成します。

ロード バランシングは、VPN クラスタ内の 2 台以上の ASA 間で、VPN トラフィックを分散します。

ネットワーク アクセス コントロール（NAC）は、ネットワークへの本番アクセスの条件としてエンドポイントの準拠性チェックと脆弱性チェックを実行することにより、ワーム、ウイルス、および不正アプリケーションによる侵入および感染からエンタープライズのネットワークを保護します。これらのチェックは、*ポスチャ検証* と呼ばれます。

インターフェイスでの IKE のイネーブル化

IKE を使用するには、使用する予定のインターフェイスごとに、IKE をイネーブルにする必要があります。

VPN 接続の場合

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。

ステップ 2　[Access Interfaces] 領域で、IKE を使用するインターフェイスに対して、[IPsec (IKEv2) Access] の下にある [Allow Access] をオンにします。

サイト間 VPN の場合

ステップ 1　ASDM で、[Configuration] > [Site-to-Site VPN] > [Connection Profiles] を選択します。

ステップ 2　IKEv1 および IKEv2 を使用するインターフェイスを選択します。

サイト間 VPN の IKE パラメータの設定

IKE パラメータ

ASDM で、[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Parameters] を選択します。

NAT の透過性

[Enable IPsec over NAT-T]

IPsec over NAT-T により IPSec ピアは、リモート アクセスと LAN-to-LAN の両方の接続を NAT デバイスを介して確立できます。NAT-T は UDP データグラムの IPsec トラフィックをカプセル化し、ポート 4500 を使用して、NAT デバイスにポート情報を提供します。NAT-T はすべての NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。この機能は、デフォルトでイネーブルにされています。

- ASA は、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-T、および IPSec over UDP を同時にサポートできます。
- NAT-T と IPsec over UDP の両方がイネーブルになっている場合、NAT-T が優先されます。
- イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

ASA による NAT-T の実装では、次の場合において、単一の NAT/PAT デバイスの背後にある IPSec ピアをサポートします。

- LAN-to-LAN 接続。
- LAN-to-LAN 接続または複数のリモート アクセス クライアントのいずれか。ただし、両方を混在させることはできません。

NAT-T を使用するには、次の手順を実行する必要があります。

- ポート 4500 を開くために使用するインターフェイスの ACL を作成します（[Configuration] > [Firewall] > [Access Rules]）。
- このペインで、IPSec over NAT-T をイネーブルにします。
- [Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Prefragmentation Policies] ペインのフラグメンテーション ポリシー パラメータで、[Enable IPsec Pre-fragmentation] で使用するインターフェイスを編集します。これが設定されている場合、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが移動できます。これによって、IP フラグメンテーションをサポートする NAT デバイスの動作が妨げられることはありません。

[Enable IPsec over TCP]

IPSec over TCP を使用すると、標準 ESP や標準 IKE が機能できない環境、または既存のファイアウォール ルールを変更した場合に限って機能できる環境で、VPN クライアントが動作可能になります。IPSec over TCP は TCP パケット内で IKE プロトコルと IPSec プロトコルをカプセル化し、NAT と PAT の両方のデバイスおよびファイアウォールによりセキュアなトンネリングを実現します。この機能はデフォルトで無効に設定されています。

（注）　この機能は、プロキシベースのファイアウォールでは動作しません。

IPsec over TCP は、リモート アクセス クライアントで動作します。また、すべての物理インターフェイスと VLAN インターフェイスでも動作します。これは、ASA 機能に対応するクライアントに限られます。LAN-to-LAN 接続では機能しません。

- ASA は、データ交換を行うクライアントに応じて、標準の IPsec、IPsec over TCP、NAT-Traversal、および IPsec over UDP を同時にサポートできます。
- 1 度に 1 つのトンネルをサポートする VPN 3002 ハードウェア クライアントは、標準の IPsec、IPsec over TCP、NAT-Traversal、または IPsec over UDP を使用して接続できます。
- イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

ASA とその接続先のクライアントの両方で IPsec over TCP をイネーブルにします。

最大 10 個のポートを指定して、それらのポートに対して IPsec over TCP をイネーブルにできます。ポート 80（HTTP）やポート 443（HTTPS）などのウェルノウン ポートを入力すると、そのポートに関連付けられているプロトコルが機能しなくなることを示す警告がシステムに表示されます。その結果、ブラウザを使用して、IKE がイネーブルのインターフェイスから ASA を管理することができなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

ASA だけでなく、クライアントでも TCP ポートを設定する必要があります。クライアントの設定には、ASA 用に設定したポートを少なくとも 1 つ含める必要があります。

ピアに送信される ID

IKE ネゴシエーションでピアが相互に相手を識別する [Identity] を選択します。

Address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
Hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
Key ID	リモート ピアが事前共有キーを検索するために使用する [Key Id String] を指定します。
Automatic	接続タイプによって IKE ネゴシエーションを決定します。 • 事前共有キーの IP アドレス • 証明書認証の cert DN。

セッション制御

[Disable Inbound Aggressive Mode Connections]

フェーズ 1 の IKE ネゴシエーションでは、Main モードと Aggressive モードのいずれかを使用できます。どちらのモードも同じサービスを提供しますが、Aggressive モードの場合にピア間で必要とされる交換処理は、3 つではなく 2 つだけです。Agressive モードの方が高速ですが、通信パーティの ID は保護されません。そのため、情報を暗号化するセキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。この機能はデフォルトで無効に設定されています。

[Alert Peers Before Disconnecting]

ASA のシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、または管理者による停止などのいくつかの理由で、クライアント セッションまたは LAN-to-LAN セッションがドロップすることがあります。

ASA は、（LAN-to-LAN コンフィギュレーションの場合）限定されたピアである VPN クライアントと VPN 3002 ハードウェア クライアントに、セッションが接続解除される直前に通知し、その理由を伝えることができます。アラートを受信したピアまたはクライアントは、その理由を復号化してイベント ログまたはポップアップ ペインに表示します。この機能はデフォルトで無効に設定されています。

このペインでは、ASA がそれらのアラートを送信し、接続解除の理由を伝えることができるように、通知機能をイネーブルにすることができます。

限定されたクライアントとピアには次のものが含まれます。

- アラートがイネーブルになっているセキュリティ アプライアンス
- バージョン 4.0 以降のソフトウェアを実行している VPN クライアント（設定は不要）。
- 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3002 ハードウェア クライアント。
- 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3000 シリーズ コンセントレータ

[Wait for All Active Sessions to Voluntarily Terminate Before Rebooting]

すべてのアクティブ セッションが自発的に終了した場合に限り、ASA がリブートするようにスケジュールを設定できます。この機能はデフォルトで無効に設定されています。

[Number of SAs Allowed in Negotiation for IKEv1]

一時点でのネゴシエーション中 SA の総数を制限します。

IKE v2 特有の設定

追加のセッション制御は、オープン SA の数を制限する IKE v2 で使用できます。デフォルトでは、ASA はオープン SA の数を制限しません。

- [Cookie Challenge]：選択すると、SA 初期パケットへの応答として、ASA からクッキー チャレンジがピア デバイスに送信されるようになります。
  - [% threshold before incoming SAs are cookie challenged]：ASA に対して許可される SA の総数のうち、ネゴシエーション中であるものの割合（%）。この数に達すると、以降の SA ネゴシエーションに対してクッキー チャレンジが行われます。範囲は 0 ～ 100 % です。デフォルト値は 50 % です。
- [Number of Allowed SAs in Negotiation]：一時点でのネゴシエーション中 SA の総数を制限します。クッキー チャレンジと併用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこの制限よりも低くしてください。
- [Maximum Number of SAs Allowed]：ASA 上で許可される IKEv2 接続の数を制限します。デフォルトでは、ライセンスで指定されている最大接続数が上限です。

[Preventing DoS Attacks with IKE v2 Specific Settings]

着信セキュリティ アソシエーション（SA）識別のチャレンジを行うクッキー チャレンジを設定するか、オープンな SA の数を制限することにより、IPsec IKEv2 接続に対するサービス拒否（DoS）攻撃を防止できます。デフォルトでは、ASA は、オープンな SA の数を制限せず、SA のクッキー チャレンジを行うことはありません。許可される SA の数を制限することもできます。これによって、それ以降は接続のネゴシエーションが行われなくなるため、クッキー チャレンジ機能では阻止できず現在の接続を保護できない可能性がある、メモリや CPU への攻撃を防止できます。

DoS 攻撃では、攻撃者が攻撃を開始すると、ピア デバイスから SA 初期パケットが送信され、ASA からその応答が送信されますが、ピア デバイスからのそれ以降の応答が停止されます。ピア デバイスがこれを継続的に行うと、許可されている数の SA 要求が使い果たされてしまい、最終的に ASA が応答を停止してしまうことがあります。

クッキー チャレンジのしきい値（%）をイネーブルにすると、オープン SA ネゴシエーションの数が制限されます。たとえば、デフォルト設定の 50 % では、許可される SA の 50 % がネゴシエーション中（オープン）のときに、ASA は、それ以降到着した SA 初期パケットに対してクッキー チャレンジを行います。10,000 個の IKEv2 SA が許可される Cisco ASA 5585-X では、5000 個の SA がオープンになると、それ以降の着信 SA に対してクッキー チャレンジが行われます。

[Number of SAs Allowed in Negotiation]、または [Maximum Number of SAs Allowed] とともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこれらの設定よりも低くしてください。

[Configuration] > [Site-to-Site VPN] > [Advanced] > [System Options] を選択して、IPsec レベルのすべての SA の寿命を制限することもできます。

IKE ポリシーの作成

IKE の概要

各 IKE ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。

フェーズ 1 は、以後の IKE ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 では、データを保護するトンネルが作成されます。

IKE ネゴシエーションの条件を設定するには、次に示す項目を含む IKE ポリシーを 1 つ以上作成します。

- 一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。
- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- HMAC 方式。送信者の身元を保証し、搬送中にメッセージが変更されていないことを保証します。
- 暗号キー判別アルゴリズムを強化する Diffie-Hellman グループ。このアルゴリズムを使用して、ASA は暗号キーとハッシュ キーを導出します。
- ASA が暗号キーを置き換える前に、この暗号キーを使用する最長時間の制限。

IKEv1 の場合は、各パラメータに対して 1 つの設定だけをイネーブルにできます。IKEv2 の場合は、1 つのプロポーザルで複数の設定（[Encryption]、[D-H Group]、[Integrity Hash]、および [PRF Hash]）を指定できます。

IKE ポリシーが何も設定されていない場合、ASA はデフォルトのポリシーを使用します。デフォルト ポリシーは常にプライオリティが最も低く設定され、各パラメータはデフォルト値に設定されます。特定のパラメータの値を指定しない場合、デフォルト値が適用されます。

IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。

暗号化、ハッシュ、認証、および Diffie-Hellman の値が同じで、SA ライフタイムが送信されたポリシーのライフタイム以下の場合には、IKE ポリシー間に一致が存在します。ライフタイムが等しくない場合は、（リモート ピア ポリシーからの）短い方のライフタイムが適用されます。一致するポリシーがない場合、IKE はネゴシエーションを拒否し、IKE SA は確立されません。

IKE ポリシーの設定

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec > IKE Policies]

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Policies]

フィールド

- [IKEv1 Policies]：設定済み IKE ポリシーそれぞれのパラメータ設定を表示します。
  - [Priority #]：ポリシーのプライオリティを示します。
  - [Encryption]：暗号化方式を示します。
  - [Hash]：ハッシュ アルゴリズムを示します。
  - [D-H Group]：Diffie-Hellman グループを示します。
  - [Authentication]：認証方式を示します。
  - [Lifetime (secs)]：SA ライフタイムを秒数で示します。
- [Add]/[Edit]/[Delete]：IKEv1 ポリシーを追加、編集、または削除するときにクリックします。
- [IKEv2 Policies]：設定済み IKEv2 ポリシーそれぞれのパラメータ設定を表示します。
  - [Priority #]：ポリシーのプライオリティを示します。
  - [Encryption]：暗号化方式を示します。
  - [Integrity Hash]：ハッシュ アルゴリズムを示します。
  - [PRF Hash]：疑似乱数関数（PRF）ハッシュ アルゴリズムを示します。
  - [D-H Group]：Diffie-Hellman グループを示します。
  - [Lifetime (secs)]：SA ライフタイムを秒数で示します。
- [Add]/[Edit]/[Delete]：IKEv2 ポリシーを追加、編集、または削除するときにクリックします。

IKEv1 ポリシーの追加

[Configuration] > [VPN] > [IKE] > [Policies] > [Add/Edit IKEv1 Policy]

フィールド

[Priority #]：IKE ポリシーのプライオリティを設定する数字を入力します。範囲は 1 ～ 65535 で、1 が最高のプライオリティです。

[Encryption]：暗号化方式を選択します。これは、2 つの IPSec ピア間で伝送されるデータを保護する対称暗号化アルゴリズムです。次の中から選択できます。

des	56 ビット DES-CBC。安全性は低いですが、他の選択肢より高速です。デフォルト。
3des	168 ビット Triple DES。
aes	128 ビット AES。
aes-192	192 ビット AES。
aes-256	256 ビット AES。

[Hash]：データの整合性を保証するハッシュ アルゴリズムを選択します。パケットが、そのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。

sha	SHA-1	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
md5	MD5	

[Authentication]：各 IPSec ピアの ID を確立するために ASA が使用する認証方式を選択します。事前共有キーは拡大するネットワークに対応した拡張が困難ですが、小規模ネットワークではセットアップが容易です。次の選択肢があります。

pre-share	事前共有キー。
rsa-sig	RSA シグニチャ アルゴリズムによって生成されたキー付きのデジタル証明書。
crack	モバイル IPSec がイネーブルになっているクライアントの IKE Challenge/Response for Authenticated Cryptographic Keys プロトコル。証明書以外の認証技術を使用します。

[D-H Group]：Diffie-Hellman グループ ID を選択します。この ID は、2 つの IPSec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。

1	グループ 1（768 ビット）	デフォルトの Group 2（1024 ビット Diffie-Hellman）は、Group 1 または 5 と比較して、CPU の実行時間は短いですが、安全性は低くなります。
2	グループ 2（1024 ビット）	
5	グループ 5（1536 ビット）	

[Lifetime (secs)]：[Unlimited] をオンにするか、SA ライフタイムを整数で入力します。デフォルトは 86,400 秒、つまり 24 時間です。ライフタイムを長くするほど、ASA は以後の IPSec セキュリティ アソシエーションをより緩やかにセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

[Time Measure]：時間基準を選択します。ASA では、次の値を使用できます。

120 ～ 86,400 秒

2 ～ 1,440 分

1 ～ 24 時間

1 日

IKEv2 ポリシーの追加

[Configuration] > [VPN] > [IKE] > [Policies] > [Add/Edit IKEv2 Policy]

フィールド

[Priority #] : IKEv2 ポリシーのプライオリティを設定する数字を入力します。範囲は 1 ～ 65535 で、1 が最高のプライオリティです。

[Encryption] : 暗号化方式を選択します。これは、2 つの IPSec ピア間で伝送されるデータを保護する対称暗号化アルゴリズムです。次の中から選択できます。

des	56 ビット DES-CBC 暗号化を ESP に対して指定します。
3des	（デフォルト）トリプル DES 暗号化アルゴリズムを ESP に対して指定します。
aes	AES と 128 ビット キー暗号化を ESP に対して指定します。
aes-192	AES と 192 ビット キー暗号化を ESP に対して指定します。
aes-256	AES と 256 ビット キー暗号化を ESP に対して指定します。
aes-gcm	AES-GCM/GMAC 128 ビットのサポートを対称暗号化と整合性に対して指定します。
aes-gcm-192	AES-GCM/GMAC 192 ビットのサポートを対称暗号化と整合性に対して指定します。
aes-gcm-256	AES-GCM/GMAC 256 ビットのサポートを対称暗号化と整合性に対して指定します。
NULL	暗号化が行われないことを示します。

[D-H Group] : Diffie-Hellman グループ ID を選択します。この ID は、2 つの IPSec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。

1	グループ 1（768 ビット）	デフォルトの Group 2（1024 ビット Diffie-Hellman）は、Group 2 または 5 と比較して、CPU の実行時間は短いですが、安全性は低くなります。
2	グループ 2（1024 ビット）	
5	グループ 5（1536 ビット）	
14	グループ 14	
19	グループ 19	
20	グループ 20	
21	グループ 21	
24	グループ 24	

[Integrity Hash]：ESP プロトコルのデータ整合性を保証するためのハッシュ アルゴリズムを選択します。パケットが、そのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。

sha	SHA 1	デフォルトは SHA 1 です。MD5 の方がダイジェストが小さく、SHA 1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
md5	MD5	
sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha384	**SHA 2、384 ビットのダイジェスト**	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha512	**SHA 2、512 ビットのダイジェスト**	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
null		AES-GCM または AES-GMAC が暗号化アルゴリズムとして設定されていることを示します。AES-GCM が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

[Pseudo-Random Function (PRF)]：SA で使用されるすべての暗号化アルゴリズムのためのキー関連情報の組み立てに使用される PRF を指定します。

sha	SHA-1	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
md5	MD5	
sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。

[Lifetime (secs)]：[Unlimited] をオンにするか、SA ライフタイムを整数で入力します。デフォルトは 86,400 秒、つまり 24 時間です。ライフタイムを長くするほど、ASA は以後の IPSec セキュリティ アソシエーションをより迅速にセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

ASA では、次の値を使用できます。

120 ～ 86,400 秒

2 ～ 1,440 分

1 ～ 24 時間

1 日

[Assignment Policy]

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy]

[Assignment Policy] は、IP アドレスがリモート アクセス クライアントに割り当てられる方法を設定します。

フィールド

- [Use authentication server]：認証サーバから取得した IP アドレスをユーザ単位で割り当てる場合に選択します。IP アドレスが設定された認証サーバ（外部または内部）を使用している場合は、この方式を使用することを推奨します。許可サーバは、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] ペインで設定されます。
- [Use DHCP]：DHCP サーバから IP アドレスを取得する場合に選択します。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。
- [Use internal address pools]：ASA により、内部で設定されたプールから IP アドレスを割り当てる場合に選択します。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。
  - [Allow the reuse of an IP address __ 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。遅延を追加する場合は、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。

IPsec の設定

ASA では、IPsec は LAN-to-LAN VPN 接続に使用され、client-to-LAN VPN 接続にも IPsec を使用できます。IPsec 用語では、「ピア」とは、リモート アクセス クライアントまたは別のセキュアなゲートウェイを意味します。

（注） ASA は、シスコのピア（IPv4 または IPv6）や、関連するすべての標準に準拠したサードパーティのピアとの LAN-to-LAN IPsec 接続をサポートしています。

トンネルを確立する間に、2 つのピアは、認証、暗号化、カプセル化、キー管理を制御するセキュリティ アソシエーションをネゴシエートします。これらのネゴシエーションには、トンネルの確立（IKE SA）と、トンネル内のトラフィックの制御（IPsec SA）という 2 つのフェーズが含まれます。

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。IPsec LAN-to-LAN 接続では、ASA は発信側または応答側として機能します。IPsec client-to-LAN 接続では、ASA は応答側としてだけ機能します。発信側は SA を提案し、応答側は、設定された SA パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

ASA は、次の IPSec 属性をサポートします。

- 認証でデジタル証明書を使用するときに、フェーズ 1 ISAKMP セキュリティ アソシエーションをネゴシエートする場合の Main モード
- 認証で事前共有キーを使用するときに、フェーズ 1 ISAKMP セキュリティ アソシエーション（SA）をネゴシエートする場合の Aggressive モード
- 認証アルゴリズム：
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- 認証モード：
  - 事前共有キー
  - X.509 デジタル証明書
- Diffie-Hellman Group 1、2、および 5
- 暗号化アルゴリズム：
  - AES-128、-192、および -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- 拡張認証（XAuth）
- モード コンフィギュレーション（別名 ISAKMP コンフィギュレーション方式）
- トンネル カプセル化モード
- LZS を使用した IP 圧縮（IPCOMP）

クリプト マップの追加

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps]

このペインには、IPSec ルールに定義されている、現在設定されているクリプト マップが表示されます。ここでは、IPSec ルールを追加、編集、削除、切り取り、および貼り付けしたり、上下に移動させたりできます。

フィールド

（注） 暗黙のルールは、編集、削除、またはコピーできません。ASA は、ダイナミック トンネル ポリシーが設定されている場合、リモート クライアントからトラフィックの選択提案を暗黙的に受け入れます。特定のトラフィックを選択することによって、その提案を無効化できます。

- [Add]：[Create IPSec Rule] が開きます。このダイアログボックスでは、ルールの基本、詳細、およびトラフィックの選択パラメータを設定できます。
- [Edit]：既存のルールを編集します。
- [Delete]：テーブルで選択したルールを削除します。
- [Cut]：テーブルで選択したルールを切り取り、コピーできるようにクリップボードに保持します。

- [Copy]：テーブルで選択したルールをコピーします。
- [Find]：検索する既存ルールのパラメータを指定するための [Find] ツールバーをイネーブルにします。
  - [Filter]：[is] または [contains] を選択し、フィルタ パラメータを入力することによって、Interface、Source、Destination Service、または Rule Query を基準にして検索結果をフィルタリングします。[...] をクリックして、選択可能なすべての既存エントリが示された参照ダイアログボックスを開きます。
- [Diagram]：選択した IPSec ルールを示す図を表示します。
- [Type: Priority]：ルールのタイプ（Static または Dynamic）とそのプライオリティを表示します。
- Traffic Selection
  - [#]：ルール番号を示します。
  - [Source]：トラフィックを [Remote Side Host/Network] カラムのリストにある IP アドレス宛てに送信するときに、このルールに従う IP アドレスを示します。詳細モード（[Show Detail] ボタンを参照）では、アドレス カラムに、単語 any が付いたインターフェイス名が含まれることがあります（inside: any など）。any とは、内部インターフェイスにある任意のホストが、ルールによって影響を受けることを意味します。
  - [Destination]：トラフィックが [Security Appliance Side Host/Network] カラムのリストにある IP アドレスから送信されるときに、このルールに従う IP アドレスを一覧表示します。詳細モード（[Show Detail] オプション ボタンを参照）では、アドレス カラムに、単語 any が付いたインターフェイス名が含まれることがあります（outside: any など）。any とは、外部インターフェイスにある任意のホストが、ルールによって影響を受けることを意味します。さらに詳細モードでは、アドレス カラムに角カッコで囲まれた IP アドレスが含まれることもあります（[209.165.201.1-209.165.201.30] など）。これらのアドレスは、変換済みアドレスです。内部ホストが外部ホストへの接続を作成すると、ASA は内部ホストのアドレスをプールのアドレスにマッピングします。ホストがアウトバウンド接続を作成した後、ASA はこのアドレス マッピングを維持します。このアドレス マッピング構造は xlate と呼ばれ、一定の時間メモリに保持されます。
  - [Service]：ルールによって指定されるサービスとプロトコルを指定します（TCP、UDP、ICMP、または IP）。
  - [Action]：IPSec ルールのタイプ（保護する、または保護しない）を指定します。
- [Transform Set]：ルールのトランスフォーム セットを表示します。
- [Peer]：IPsec ピアを識別します。
- [PFS]：ルールの完全転送秘密設定値を表示します。
- [NAT-T Enabled]：ポリシーで NAT Traversal が有効になっているかどうかを示します。
- [Reverse Route Enabled]：ポリシーで逆ルート注入がイネーブルになっているかどうかを示します。
- [Connection Type]：（スタティック トンネルの場合にだけ該当）このポリシーの接続タイプを、bidirectional、originate-only、または answer-only として識別します。
- [SA Lifetime]：ルールの SA ライフタイムを表示します。
- [CA Certificate]：ポリシーの CA 証明書を表示します。これは、スタティック接続にだけ適用されます。
- [IKE Negotiation Mode]：IKE ネゴシエーションで、Main モードまたは Aggressive モードを使用するかどうかを表示します。

- [Description]：（オプション）このルールの簡単な説明を指定します。既存ルールの場合は、ルールの追加時に入力した説明になります。暗黙のルールには「Implicit rule」という説明が加えられます。暗黙のルール以外のルールの説明を編集するには、このカラムを右クリックして [Edit Description] を選択するか、またはカラムをダブルクリックします。
- [Enable Anti-replay window size]：アンチ リプレイ ウィンドウのサイズを、64 ～ 1028 の範囲の 64 の倍数で設定します。トラフィック シェーピングを使用する、階層型 QoS ポリシーにおけるプライオリティ キューイング（「[Rule Actions] > [QoS] タブ」を参照）に伴う副次的な影響としては、パケットの順番が変わる点が挙げられます。IPsec パケットでは、アンチ リプレイ ウィンドウ内にない不連続パケットにより、警告 syslog メッセージが生成されます。これらの警告は、プライオリティ キューイングの場合は誤報です。リプレイ攻撃防止のパネル サイズを設定すると、誤報を回避することができます。

IPsec ルールの作成：[Tunnel Policy (Crypto Map) - Basic] タブ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps] : [Edit IPsec Rule] : [Basic] タブ

このペインでは、IPSec ルールの新しいトンネル ポリシーを定義します。ここで定義する値は、[OK] をクリックした後に [IPSec Rules] テーブルに表示されます。すべてのルールは、デフォルトで [IPSec Rules] テーブルに表示されるとすぐにイネーブルになります。

[Tunnel Policy] ペインでは、IPSec（フェーズ 2）セキュリティ アソシエーション（SA）のネゴシエートで使用するトンネル ポリシーを定義できます。ASDM は、ユーザのコンフィギュレーション編集結果を取り込みますが、[Apply] をクリックするまでは実行中のコンフィギュレーションに保存しません。

すべてのトンネル ポリシーでは、トランスフォーム セットを指定し、適用するセキュリティ アプライアンス インターフェイスを特定する必要があります。トランスフォーム セットでは、IPSec の暗号化処理と復号化処理を実行する暗号化アルゴリズムおよびハッシュ アルゴリズムを特定します。すべての IPSec ピアが同じアルゴリズムをサポートするとは限らないため、多くのポリシーを指定して、それぞれに 1 つのプライオリティを割り当てるようにすることもできます。その後セキュリティ アプライアンスは、リモートの IPSec ピアとネゴシエートして、両方のピアがサポートするトランスフォーム セットを一致させます。

トンネル ポリシーは、*スタティック*または*ダイナミック*にすることができます。スタティック トンネル ポリシーでは、セキュリティ アプライアンスで IPSec 接続を許可する 1 つ以上のリモート IPSec ピアまたはサブネットワークを特定します。スタティック ポリシーを使用して、セキュリティ アプライアンスで接続を開始するか、またはリモート ホストから接続要求を受信するかどうかを指定できます。スタティック ポリシーでは、許可されるホストまたはネットワークを識別するために必要な情報を入力する必要があります。

ダイナミック トンネル ポリシーは、セキュリティ アプライアンスとの接続を開始することを許可されるリモート ホストについての情報を指定できないか、または指定しない場合に使用します。リモート VPN 中央サイト デバイスとの関係で、セキュリティ アプライアンスを VPN クライアントとしてしか使用しない場合は、ダイナミック トンネル ポリシーを設定する必要はありません。ダイナミック トンネル ポリシーが最も効果的なのは、リモート アクセス クライアントが、VPN 中央サイト デバイスとして動作するセキュリティ アプライアンスからユーザ ネットワークへの接続を開始できるようにする場合です。ダイナミック トンネル ポリシーは、リモート アクセス クライアントにダイナミックに割り当てられた IP アドレスがある場合、または多くのリモート アクセス クライアントに別々のポリシーを設定しないようにする場合に役立ちます。

フィールド

- [Interface]：このポリシーを適用するインターフェイス名を選択します。
- [Policy Type]：このトンネル ポリシーのタイプとして、[Static] または [Dynamic] を選択します。
- [Priority]：ポリシーのプライオリティを入力します。
- [IKE Proposals (Transform Sets)]：IKEv1 および IKEv2 の IPsec プロポーザルを指定します。
  - [IKEv1 IPsec Proposal]：ポリシーのプロポーザル（トランスフォーム セット）を選択して [Add] をクリックすると、アクティブなトランスフォーム セットのリストに移動します。[Move Up] または [Move Down] をクリックして、リスト ボックス内でのプロポーザルの順番を入れ替えます。クリプト マップ エントリまたはダイナミック クリプト マップ エントリには、最大で 11 のプロポーザルを追加できます。
  - [IKEv2 IPsec Proposal]：ポリシーのプロポーザル（トランスフォーム セット）を選択して [Add] をクリックすると、アクティブなトランスフォーム セットのリストに移動します。[Move Up] または [Move Down] をクリックして、リスト ボックス内でのプロポーザルの順番を入れ替えます。クリプト マップ エントリまたはダイナミック クリプト マップ エントリには、最大で 11 のプロポーザルを追加できます。
- [Peer Settings - Optional for Dynamic Crypto Map Entries]：ポリシーのピア設定値を設定します。
  - [Connection Type]：（スタティック トンネルの場合にだけ該当）このポリシーの接続タイプを、bidirectional、originate-only、または answer-only から選択します。LAN-to-LAN 接続の場合は、bidirectional または answer-only（originate-only ではない）を選択します。LAN-to-LAN 冗長接続の場合は、answer-only を選択します。originate only を選択した場合は、最大 10 個の冗長ピアを指定できます。単方向に対してだけ、originate only または answer only を指定できます。どちらもデフォルトでイネーブルになっていません。
  - [IP Address of Peer to Be Added]：追加する IPSec ピアの IP アドレスを入力します。
- [Enable Perfect Forwarding Secrecy]：ポリシーの PFS をイネーブルにする場合にオンにします。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPSec ネゴシエーションでのフェーズ 2 キーは、PFS を指定しない限りフェーズ 1 に基づいて生成されます。
- [Diffie-Hellman Group]：PFS をイネーブルにする場合は、ASA がセッション キーの生成に使用する Diffie-Hellman グループも選択する必要があります。次の選択肢があります。
  - [Group 1（768 ビット）]：PFS を使用し、Diffie-Hellman Group 1 を使用して IPSec セッション キーを生成します。このときの素数と generator 数は 768 ビットです。このオプションは高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
  - [Group 2（1024 ビット）]：PFS を使用し、Diffie-Hellman Group 2 を使用して IPSec セッション キーを生成します。このときの素数と generator 数は 1024 ビットです。このオプションは Group 1 より高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
  - [Group 5（1536 ビット）]：PFS を使用し、Diffie-Hellman Group 5 を使用して IPSec セッション キーを生成します。このときの素数と generator 数は 1536 ビットです。このオプションは Group 2 より高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
  - [Group 14]：完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 14 を使用します。
  - [Group 19]：完全転送秘密を使用し、IKEv2 に対する Diffie-Hellman グループ 19 を使用して、ECDH をサポートします。

- [Group 20]：完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 20 を使用して、ECDH をサポートします。
- [Group 21]：完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 21 を使用して、ECDH をサポートします。
- [Group 24]：完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 24 を使用します。

IPsec ルールの作成：[Tunnel Policy (Crypto Map) - Advanced] タブ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps]：[Edit IPsec Rule]：[Advanced] タブ

フィールド

- [Enable NAT-T]：このポリシーの NAT Traversal（NAT-T）をイネーブルにします。
- [Enable Reverse Route Injection]：このポリシーの逆ルート注入をイネーブルにします。逆ルート注入（RRI）は、ダイナミック ルーティング プロトコルを使用する内部ルータのルーティング テーブルにデータを入力するために使用されます。ダイナミック ルーティング プロトコルの例としては、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）（ASA を実行する場合）、ルーティング情報プロトコル（RIP）（リモート VPN クライアントや LAN-to-LAN セッションに使用）があります。
- [Security Association Lifetime Settings]：セキュリティ アソシエーション（SA）の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
  - [Time]：時（hh）、分（mm）、および秒（ss）単位で SA のライフタイムを指定します。
  - [Traffic Volume]：キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロード データのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。
- [Static Type Only Settings]：スタティック トンネル ポリシーのパラメータを指定します。
  - [Device Certificate]：使用する証明書を選択します。デフォルトの [None]（事前共有キーを使用）以外の値を選択する場合。[None] 以外を選択すると、[Send CA certificate chain] チェックボックスがオンになります。
  - [Send CA certificate chain]：トラスト ポイント チェーン全体の伝送をイネーブルにします。
  - [IKE Negotiation Mode]：IKE ネゴシエーション モード（Main または Aggressive）を選択します。このパラメータにより、キー情報の交換と SA のセットアップを行う場合のモードを設定します。ネゴシエーションの発信側が使用するモードを設定し、応答側は自動ネゴシエーションします。Aggressive モードは高速で、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。Main モードは低速で、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。このモードはより安全性が高く、デフォルトで選択されています。[Aggressive] を選択すると、[Diffie-Hellman Group] リストがアクティブになります。
  - [Diffie-Hellman Group]：適用する Diffie-Hellman グループを選択します。Group 1（768 ビット）、Group 2（1024 ビット）Group 5（1536 ビット）の中から選択します。
- [ESP v3]：着信 ICMP エラー メッセージを、暗号化マップとダイナミック暗号化マップのどちらに対して検証するかを指定し、セキュリティ単位のアソシエーション ポリシーを設定するか、トラフィック フロー パケットをイネーブルにします。

- [Validate incoming ICMP error messages]：IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先のこれらの ICMP エラー メッセージを検証するかどうかを選択します。
- [Enable Do Not Fragment (DF) policy]：IP ヘッダーに Do-Not-Fragment（DF）ビット セットを持つ大きなパケットを IPSec サブシステムがどのように処理するかを定義します。次のいずれかを選択します。

  [Clear DF bit]：DF ビットを無視します。

  [Copy DF bit]：DF ビットを維持します。

  [Set DF bit]：DF ビットを設定して使用します。
- [Enable Traffic Flow Confidentiality (TFC) packets]：トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットをイネーブルにします。

  （注）　TFC をイネーブルにする前に、[Tunnel Policy (Crypto Map)] の [Basic] タブで IKE v2 IPsec プロポーザルが設定されていなければなりません。

  バースト、ペイロード サイズ、およびタイムアウト パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

IPsec ルールの作成：[Traffic Selection] タブ

[Configuration] > [VPN] > [IPsec] > [IPSec Rules] > [Add/Edit Rule] > [Tunnel Policy (Crypto Map)] : [Traffic Selection] タブ

このペインでは、保護する（許可）トラフィックまたは保護しない（拒否）トラフィックを定義できます。

フィールド

- [Action]：このルールで実行するアクションを指定します。選択肢は、[protect] と [do not protect] です。
- [Source]：送信元ホストまたはネットワークの IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。[...] をクリックして、次のフィールドを含む [Browse Source] ダイアログボックスを開きます。
  - [Add/Edit]：送信元アドレスまたはグループを追加するには、[IP Address] または [Network Object Group] を選択します。
  - [Delete]：エントリを削除します。
  - [Filter]：表示される結果をフィルタリングする IP アドレスを入力します。
  - [Name]：続くパラメータが、送信元ホストまたはネットワークの名前を指定することを示します。
  - [IP Address]：続くパラメータが、送信元ホストまたはネットワークのインターフェイス、IP アドレス、およびサブネット マスクを指定することを示します。
  - [Netmask]：IP アドレスに適用する標準サブネット マスクを選択します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
  - [Description]：説明を入力します。
  - [Selected Source]：選択したエントリを送信元として含めるには [Source] をクリックします。

- [Destination]：宛先ホストまたはネットワークの IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。[...] をクリックして、次のフィールドを含む [Browse Destination] ダイアログを開きます。
  - [Add/Edit]：[IP Address] または [Network Object Group] を選択して、宛先アドレスまたはグループを追加します。
  - [Delete]：エントリを削除します。
  - [Filter]：表示される結果をフィルタリングする IP アドレスを入力します。
  - [Name]：続くパラメータが、宛先ホストまたはネットワークの名前を指定することを示します。
  - [IP Address]：続くパラメータが、宛先ホストまたはネットワークのインターフェイス、IP アドレス、およびサブネット マスクを指定することを示します。
  - [Netmask]：IP アドレスに適用する標準サブネット マスクを選択します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
  - [Description]：説明を入力します。
  - [Selected Destination]：選択したエントリを宛先として含めるには [Destination] をクリックします。
- [Service]：サービスを入力するか、または [...] をクリックして [Browse Service] ダイアログ ボックスを開き、サービスのリストから選択できます。
- [Description]：[Traffic Selection] のエントリの説明を入力します。
- More Options
  - [Enable Rule]：このルールをイネーブルにします。
  - [Source Service]：サービスを入力するか、[...] をクリックしてサービス参照ダイアログ ボックスを開き、サービスのリストから選択します。
  - [Time Range]：このルールを適用する時間範囲を定義します。
  - [Group]：続くパラメータが、送信元ホストまたはネットワークのインターフェイスとグループ名を指定することを示します。
  - [Interface]：IP アドレスのインターフェイス名を選択します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
  - [IP address]：このポリシーが適用されるインターフェイスの IP アドレスを指定します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
  - [Destination]：送信元、宛先のホストまたはネットワークについて、IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。これらのフィールドのいずれかで [...] をクリックし、次のフィールドを含む [Browse] ダイアログボックスを開きます。
  - [Name]：送信元または宛先のホストまたはネットワークとして使用するインターフェイス名を選択します。このパラメータは、[Name] オプション ボタンを選択するときに表示されます。これは、このオプションに関連付けられる唯一のパラメータです。
  - [Interface]：IP アドレスのインターフェイス名を選択します。このパラメータは、[Group] オプション ボタンをクリックするときに表示されます。
  - [Group]：送信元または宛先のホストまたはネットワークに指定されたインターフェイスに存在するグループの名前を選択します。リストにエントリが何もない場合は、既存グループの名前を入力できます。このパラメータは、[Group] オプション ボタンをクリックするときに表示されます。
- [Protocol and Service]：このルールに関連するプロトコル パラメータとサービス パラメータを指定します。

（注）「Any - any」IPsec ルールは使用できません。このタイプのルールにより、デバイスおよびそのピアが複数の LAN-to-LAN トンネルをサポートできなくなります。

  - [TCP]：このルールを TCP 接続に適用することを指定します。これを選択すると、[Source Port] グループ ボックスと [Destination Port] グループ ボックスも表示されます。
  - [UDP]：このルールを UDP 接続に適用することを指定します。これを選択すると、[Source Port] グループ ボックスと [Destination Port] グループ ボックスも表示されます。
  - [ICMP]：このルールを ICMP 接続に適用することを指定します。これを選択すると、[ICMP Type] グループ ボックスも表示されます。
  - [IP]：このルールを IP 接続に適用することを指定します。これを選択すると、[IP Protocol] グループ ボックスも表示されます。
  - [Manage Service Groups] : [Manage Service Groups] ペインが表示され、ここで TCP/UDP サービス/ポートのグループを追加、編集、または削除できます。
  - [Source Port] および [Destination Port] : [Protocol and Service] グループ ボックスで選択したオプション ボタンに応じて、TCP または UDP のポート パラメータが表示されます。
  - [Service]：個々のサービスのパラメータを指定しようとしていることを示します。フィルタの適用時に使用するサービス名とブーリアン演算子を指定します。
  - [Boolean operator]（ラベルなし）: [Service] ボックスで指定したサービスを照合するときに使用するブーリアン条件（等号、不等号、大なり、小なり、または範囲）を一覧表示します。
  - [Service]（ラベルなし）: 照合対象のサービス（https、kerberos、その他）を指定します。range サービス演算子を指定すると、このパラメータは 2 つのボックスに変わります。ボックスに、範囲の開始値と終了値を入力します。
  - [...] : サービスのリストが表示され、ここで選択したサービスが [Service] ボックスに表示されます。
  - [Service Group] : 送信元ポートのサービス グループの名前を指定しようとしていることを示します。
  - [Service]（ラベルなし）: 使用するサービス グループを選択します。
  - [ICMP Type] : 使用する ICMP タイプを指定します。デフォルトは any です。[...] ボタンをクリックすると、使用可能なタイプのリストが表示されます。
- Options
  - [Time Range]：既存の時間範囲の名前を指定するか、新しい範囲を作成します。
  - [...] : [Add Time Range] ペインが表示され、ここで新しい時間範囲を定義できます。
  - [Please enter the description below (optional)] : ルールについて簡単な説明を入力するためのスペースです。

[Pre-Fragmentation]

[Configuration] > [VPN] > [IPsec] > [Pre-Fragmentation]

このペインでは、任意のインターフェイスの IPSec の Pre-Fragmentation ポリシーと Do-Not-Fragment（DF）ビット ポリシーを設定します。

IPSec Pre-Fragmentation ポリシーでは、パブリック インターフェイスを介してトラフィックをトンネリングするときに、最大伝送単位（MTU）の設定を超えるパケットの処理方法を指定します。この機能により、ASA とクライアントの間のルータまたは NAT デバイスが IP フラグメントを拒否またはドロップする場合に対処できます。たとえば、クライアントが ASA の背後の FTP サーバに対して FTP get コマンドを実行するとします。FTP サーバから送信されるパケットは、カプセル化されたときにパブリック インターフェイス上の ASA の MTU サイズを超過します。選択したオプションにより、ASA でのこれらのパケットの処理方法が決まります。事前フラグメンテーション ポリシーは、ASA のパブリック インターフェイスから送出されるすべてのトラフィックに適用されます。

ASA は、トンネリングされたすべてのパケットをカプセル化します。カプセル化した後、ASA は、パブリック インターフェイスから送信する前に MTU の設定値を超えるパケットをフラグメント化します。これがデフォルトのポリシーです。このオプションは、フラグメント化されたパケットが、障害なしでトンネル通過を許可される状況で機能します。FTP の例では、大きなパケットがカプセル化されてから、IP レイヤでフラグメント化されます。中間デバイスは、フラグメントをドロップするか、または異常なフラグメントだけをドロップします。ロードバランシング デバイスが、異常フラグメントを取り入れる可能性があります。

事前フラグメンテーションをイネーブルにすると、ASA は、MTU の設定値を超えるトンネリングされたパケットをカプセル化する前に、フラグメント化します。これらのパケットで DF ビットが設定されている場合、ASA は DF ビットをクリアし、パケットをフラグメント化してからカプセル化します。このアクションにより、パブリック インターフェイスを離れる 2 つの独立した非フラグメント化 IP パケットが作成され、ピア サイトで再構成される完全なパケットにフラグメントを変換することにより、これらのパケットがピア サイトに正常に伝送されます。ここでの例では、ASA が MTU を無効にし、DF ビットをクリアすることによってフラグメンテーションを許可します。

（注） *いずれの*インターフェイスであっても、[MTU] または [Pre-Fragmentation] オプションを変更すると、*すべての*既存接続が切断されます。たとえば、パブリック インターフェイスで 100 件のアクティブなトンネルが終了し、そのときに外部インターフェイスで [MTU] または [Pre-Fragmentation] オプションを変更すると、パブリック インターフェイスのすべてのアクティブなトンネルがドロップされます。

フィールド

- [Pre-Fragmentation]：設定済みインターフェイスごとに、現在の事前フラグメンテーションの設定を示します。
  - [Interface]：設定済みインターフェイスの名前を示します。
  - [Pre-Fragmentation Enabled]：インターフェイスごとに、事前フラグメンテーションがイネーブルになっているかどうかを示します。
  - [DF Bit Policy]：各インターフェイスの DF ビット ポリシーを示します。
- [Edit]：[Edit IPsec Pre-Fragmentation Policy] ダイアログボックスを表示します。

[Edit IPSec Pre-Fragmentation Policy]

[Configuration] > [VPN] > [IPsec] > [Pre-Fragmentation] > [Edit IPSec Pre-Fragmentation Policy]

このペインでは、親ペイン（[Configuration] > [VPN] > [IPSec] > [Pre-Fragmentation]）で選択したインターフェイスの、既存の IPSec 事前フラグメンテーション ポリシーと Do-Not-Fragment（DF）ビット ポリシーを変更します。

フィールド

- [Interface]：選択されたインターフェイスの名前を識別します。このダイアログボックスを使用しても、このパラメータは変更できません。
- [Enable IPsec pre-fragmentation]：IPSec の事前フラグメンテーションをイネーブルまたはディセーブルにします。ASA は、カプセル化する前に、MTU の設定を超えるトンネリングされたパケットをフラグメント化します。これらのパケットで DF ビットが設定されている場合、ASA は DF ビットをクリアし、パケットをフラグメント化してからカプセル化します。このアクションにより、パブリック インターフェイスを離れる 2 つの独立した非フラグメント化 IP パケットが作成され、ピア サイトで再構成される完全なパケットにフラグメントを変換することにより、これらのパケットがピア サイトに正常に伝送されます。
- [DF Bit Setting Policy]：Do-Not-Fragment ビット ポリシー（[Copy]、[Clear]、または [Set]）を選択します。

IPSec Transform Sets

[Configuration] > [VPN] > [IPsec] > [Transform Sets]

このペインでは、トランスフォーム セットを表示、追加、または編集します。トランスフォームは、データ フローで実行される操作のセットで、データ認証、データ機密性、およびデータ圧縮を実現します。たとえば、1 つのトランスフォームは、3DES 暗号化と HMAC-MD5 認証アルゴリズム（ESP-3DES-MD5）による ESP プロトコルです。

フィールド

- [IKEv1 IPsec Proposals (Transform Sets)]：設定済みのトランスフォーム セットを示します。
  - [Name]：トランスフォーム セットの名前を示します。
  - [Mode]：トランスフォーム セットのモード（Tunnel）を示します。このパラメータにより、ESP 暗号化と認証を適用する場合のモードを指定します。言い換えると、ESP が適用されている元の IP パケットの部分を指定します。Tunnel モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、本来の送信元アドレスと宛先アドレスが隠されることになります。
  - [ESP Encryption]：トランスフォーム セットのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズムを示します。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESP は、保護されているデータをカプセル化します。
  - [ESP Authentication]：トランスフォーム セットの ESP 認証アルゴリズムを示します。
- [Add]：[Add Transform Set] ダイアログボックスが開き、ここで新しいトランスフォーム セットを追加できます。
- [Edit]：[Edit Transform Set] ダイアログボックスが開き、ここで既存のトランスフォーム セットを変更できます。
- [Delete]：選択したトランスフォーム セットを削除します。確認されず、やり直しもできません。

- [IKEv2 IPsec Proposals]：設定済みのトランスフォーム セットを示します。
  - [Name]：IKEv2 IPsec プロポーザルの名前を示します。
  - [Encryption]：IKEv2 IPsec プロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズムを示します。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESP は、保護されているデータをカプセル化します。
  - [Integrity Hash]：ESP プロトコルのデータ整合性を保証するためのハッシュ アルゴリズムを示します。パケットが想定した発信元から発信されたこと、また搬送中に変更されていることを保証します。パケットが想定した発信元から発信されたこと、また搬送中に変更されていることを保証します。AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。
- [Add]：[Add IPsec Proposal] ダイアログボックスが開き、ここで新しいプロポーザルを追加できます。
- [Edit]：[Edit IPsec Proposal] ダイアログボックスが開き、ここで既存のプロポーザルを変更できます。
- [Delete]：選択されているプロポーザルを削除します。確認されず、やり直しもできません。

IPsec プロポーザル（トランスフォーム セット）の追加または編集

[Configuration] > [VPN] > [IPsec] > [Transform Sets] > [Add/Edit IPsec_Proposal_(Transform Set)]

このペインでは、IPsec IKEv1 トランスフォーム セットを追加または変更します。トランスフォームは、データ フローで実行される操作のセットで、データ認証、データ機密性、およびデータ圧縮を実現します。たとえば、1 つのトランスフォームは、3DES 暗号化と HMAC-MD5 認証アルゴリズム（ESP-3DES-MD5）による ESP プロトコルです。

フィールド

- [Set Name]：このトランスフォーム セットの名前を指定します。
- [Properties]：このトランスフォーム セットのプロパティを設定します。これらのプロパティは、[Transform Sets] テーブルに表示されます。
  - [Mode]：トランスフォーム セットのモード（Tunnel）を示します。このフィールドは、ESP 暗号化と認証を適用する場合のモードを示します。言い換えると、ESP を適用している元の IP パケットの部分を指定します。Tunnel モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、本来の送信元アドレスと宛先アドレスが隠されることになります。
  - [ESP Encryption]：トランスフォーム セットのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズムを選択します。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESP は、保護されているデータをカプセル化します。
  - [ESP Authentication]：トランスフォーム セットの ESP 認証アルゴリズムを選択します。

（注） IPSec ESP（Encapsulating Security Payload）プロトコルでは、暗号化と認証の両方の機能が提供されます。パケット認証により、データが、データに記述されている送信元から送信されたことを保証します。これは、「データ整合性」とも呼ばれます。

IPsec プロポーザルの追加または編集

[Configuration] > [VPN] > [IPsec] > [Transform Sets] > [Add/Edit IPsec_Proposal]

このペインでは、IPsec IKEv2 プロポーザルを追加または変更します。プロポーザルは、データ フローで実行される操作の集合であり、データ認証、データ機密性、およびデータ圧縮を実現します。たとえば、1 つのプロポーザルで、ESP プロトコルと 3DES 暗号化、および HMAC-MD5 認証アルゴリズム（ESP-3DES-MD5）が指定されます。

フィールド

- **[Name]**：このプロポーザルの名前を指定します。
- **[Encryption]**：このプロポーザルのカプセル化セキュリティ プロトコル（**ESP**）を指定します。**ESP** では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。**ESP** は、保護されているデータを*カプセル化*します。
- **[Integrity Hash]**：このプロポーザルの **ESP** 認証アルゴリズムを選択します。ハッシュ アルゴリズムとは、**ESP** プロトコルのデータ整合性を保証するためのものです。パケットが、そのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。

（注） IPSec ESP（Encapsulating Security Payload）プロトコルでは、暗号化と認証の両方の機能が提供されます。パケット認証により、データが、データに記述されている送信元から送信されたことを保証します。これは、「データ整合性」とも呼ばれます。

ロード バランシングの設定

リモート クライアント コンフィギュレーションで、複数の ASA を同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。これによって、システム リソースを効率的に利用でき、パフォーマンスと可用性が向上します。

仮想クラスタの作成

ロード バランシングを実装するには、同じプライベート LAN 間ネットワーク上の複数のデバイスを、論理的に*仮想クラスタ*としてグループ化します。

セッションの負荷は、仮想クラスタ内のすべてのデバイスに分散されます。仮想クラスタ内の 1 つのデバイスである*仮想クラスタ マスター*は、着信接続要求を*バックアップ デバイス*と呼ばれる他のデバイスに転送します。仮想クラスタ マスターは、クラスタ内のすべてのデバイスをモニタし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。仮想クラスタ マスターの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。たとえば、現在の仮想クラスタ マスターで障害が発生すると、クラスタ内のバックアップ デバイスの 1 つがその役割を引き継いで、すぐに新しい仮想クラスタ マスターになります。

仮想クラスタは、外部のクライアントには 1 つの*仮想クラスタ IP アドレス*として表示されます。この IP アドレスは、特定の物理デバイスに結び付けられていません。現在の仮想クラスタ マスターに属しているため、仮想のアドレスです。接続の確立を試みている VPN クライアントは、最初にこの仮想クラスタ IP アドレスに接続します。仮想クラスタ マスターは、クラスタ内で使用できるホストのうち、最も負荷の低いホストのパブリック IP アドレスをクライアントに返します。2 回目のトランザクションで、クライアントは直接そのホストに接続します（この動作はユーザには透過的です）。仮想クラスタ マスターは、このようにしてリソース全体に均等かつ効率的にトラフィックを転送します。

クラスタ内のマシンで障害が発生すると、終了されたセッションはただちに仮想クラスタ IP アドレスに再接続できます。次に、仮想クラスタ マスターは、クラスタ内の別のアクティブ デバイスにこれらの接続を転送します。仮想クラスタ マスター自体に障害が発生した場合、クラスタ内のバックアップ デバイスが、ただちに新しい仮想セッション マスターを自動的に引き継ぎます。クラスタ内の複数のデバイスで障害が発生しても、クラスタ内のデバイスが 1 つ稼働していて使用可能である限り、ユーザはクラスタに引き続き接続できます。

ロードバランシング クラスタは、同じリリースまたは混在リリースの ASA で構成できます。ただし、次の制約があります。

- 同じリリースの ASA の両方で構成されるロードバランシング クラスタは、IPsec、AnyConnect、およびクライアントレス SSL VPN クライアントとクライアントレス セッションの組み合わせに対してロード バランシングを実行できます。
- 混在リリースの ASA または同じリリースの ASA で構成されるロードバランシング クラスタは、IPsec セッションのみをサポートできます。ただし、このようなコンフィギュレーションでは、ASA は、それぞれの IPsec のキャパシティに完全に到達しない可能性があります。「ロード バランシングとフェールオーバーの比較」（P.24）は、この状況を示しています。

Release 7.1(1) 以降、IPsec セッションと SSL VPN セッションは、クラスタ内の各デバイスが伝送する負荷を決定するときに均等にカウントまたは重み付けします。これは、ASA Release 7.0(x) ソフトウェアと VPN 3000 コンセントレータ用のロードバランシングの計算からの逸脱を意味しています。つまり、これらのプラットフォームでは、いずれも一部のハードウェア プラットフォームにおいて、IPsec セッションの負荷とは異なる SSL VPN セッションの負荷を計算する重み付けアルゴリズムを使用しています。

クラスタの仮想マスターは、クラスタのメンバにセッション要求を割り当てます。ASA は、すべてのセッション、SSL VPN または IPsec を同等と見なし、それらを同等に割り当てます。許可する IPsec セッションと SSL VPN セッションの数は、コンフィギュレーションおよびライセンスで許可されている最大数まで設定できます。

ロードバランシング クラスタで最大 10 のノードはテスト済みです。これよりクラスタが多くても機能しますが、そのようなトポロジは正式にはサポートされていません。

地理的ロード バランシング

ロード バランシング環境において DNS 解決が一定の間隔で変化する場合は、存続可能時間（TTL）の値をどのように設定するかを慎重に検討する必要があります。DNS ロード バランス設定が AnyConnect との組み合わせで適切に機能するには、マッピングを処理する ASA の名前が、その ASA が選択された時点からトンネルが完全に確立されるまでの間、同じである必要があります。所定の時間が経過してもクレデンシャルが入力されない場合は、ルックアップが再び開始して別の IP アドレスが解決済みアドレスとなることがあります。DNS のマッピング先が別の ASA に変更された後でクレデンシャルが入力された場合は、VPN トンネルの確立に失敗します。

VPN の地理的ロード バランシングでは、Cisco Global Site Selector（GSS）が使用されることがあります。GSS では DNS がロード バランシングに使用され、DNS 解決の存続可能時間（TTL）のデフォルト値は 20 秒となっています。GSS での TTL の値を大きくすると、接続失敗の確率を大幅に引き下げることができます。値を大きくすると、ユーザがクレデンシャルを入力してトンネルを確立するときの認証フェーズに十分な時間を取ることができます。

クレデンシャル入力のための時間を増やすには、「起動時接続」をディセーブルにすることも検討してください。

ロード バランシングとフェールオーバーの比較

ロード バランシングとフェールオーバーはどちらもハイ アベイラビリティ機能ですが、これらは機能も要件も異なります。場合によっては、ロード バランシングとフェールオーバーの両方を使用できます。次の項では、これらの機能の違いについて説明します。

*ロード バランシング*とは、リモート アクセス VPN トラフィックを、仮想クラスタ内のデバイス間で均等に分配するメカニズムのことです。この機能は、スループットまたはその他の要因を考慮しない単純なトラフィックの分散に基づいています。ロードバランシング クラスタは 2 つ以上のデバイスで構成され、そのうちの 1 つが仮想マスターとなり、それ以外はバックアップとなります。これらのデバイスは、完全に同じタイプである必要はなく、同じソフトウェア バージョンやコンフィギュレーションを使用する必要もありません。仮想クラスタ内のすべてのアクティブなデバイスがセッションの負荷を伝送します。ロードバランシングにより、トラフィックはクラスタ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システム リソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

*フェールオーバー*コンフィギュレーションでは、2 台の同一の ASA を、専用のフェールオーバー リンクと、ステートフル フェールオーバー リンク（オプション）で接続します。アクティブ インターフェイスおよび装置のヘルスがモニタされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。これらの条件に一致した場合は、フェールオーバーが行われます。フェールオーバーは、VPN とファイアウォールの両方のコンフィギュレーションをサポートします。

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバーをサポートします。VPN 接続は、アクティブ/スタンバイの単一ルーテッド モードでのみ実行されます。アクティブ/アクティブ フェールオーバーにはマルチ コンテキスト モードが必要であるため、VPN 接続をサポートしません。

アクティブ/アクティブ フェールオーバーでは、両方の装置がネットワーク トラフィックを渡すことができます。これは、同じ結果になる可能性がありますが、真のロード バランシングではありません。フェールオーバーが行われると、残りのアクティブ装置が、設定されたパラメータに基づいて結合されたトラフィックの通過を引き継ぎます。したがって、アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにする必要があります。

アクティブ/スタンバイ フェールオーバーでは、1 つの装置だけがトラフィックを通過させることができ、もう 1 つの装置はスタンバイ状態で待機して、トラフィックを通過させません。アクティブ/スタンバイ フェールオーバーでは、2 番目の ASA を使用して、障害の発生した装置の機能を引き継ぎます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてスタンバイ装置がアクティブ状態に変わります。アクティブになる装置が、障害の発生した装置の IP アドレス（または、トランスペアレント ファイアウォールの場合は管理 IP アドレス）および MAC アドレスを引き継いで、トラフィックの転送を開始します。現在スタンバイになっている装置が、アクティブ装置のスタンバイの IP アドレスを引き継ぎます。アクティブ装置で障害が発生すると、スタンバイ装置は、クライアント VPN トンネルを中断することなく引き継ぎます。

ロード バランシングのライセンス要件

VPN ロード バランシングを使用するには、Security Plus ライセンスを備えた ASA モデル 5512-X、または ASA モデル 5515-X 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

適格なクライアント

ロード バランシングは、次のクライアントで開始されるリモート セッションでのみ有効です。

- Cisco AnyConnect Secure Mobility Client（Release 3.0 以降）
- Cisco ASA 5505 セキュリティ アプライアンス（Easy VPN クライアントとして動作する場合）
- IKE リダイレクトをサポートする IOS EZVPN クライアント デバイス（IOS 831/871）
- クライアントレス SSL VPN（クライアントではない）

ロード バランシングは、IPsec クライアント セッションと SSL VPN クライアントおよびクライアントレス セッションで機能します。LAN-to-LAN を含む他のすべての VPN 接続タイプ（L2TP、PPTP、L2TP/IPsec）は、ロード バランシングがイネーブルになっている ASA に接続できますが、これらの接続タイプはロード バランシングには参加できません。

ロード バランシングの前提条件

- ロード バランシングを設定する前に、まず ASA でパブリック インターフェイスとプライベート インターフェイスを設定する必要があります。これを行うには、[Configuration] > [Device Setup] > [Interfaces] を選択します。
- 仮想クラスタ IP アドレスが参照するインターフェイスを事前に設定する必要があります。
- クラスタに参加するすべてのデバイスは、同じクラスタ固有の値（IP アドレス、暗号化設定、暗号キー、およびポート）を共有する必要があります。クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

証明書の確認

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。リダイレクト 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。

High Availability and Scalability Wizard を使用した VPN クラスタ ロード バランシングの設定

リモート クライアント コンフィギュレーションで、複数の ASA を同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能はロード バランシングと呼ばれ、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロード バランシングにより、システム リソースが効率的に使用され、パフォーマンスとシステム アベイラビリティが向上します。

[VPN Cluster Load Balancing Configuration] 画面を使用して、デバイスがロード バランシング クラスタに参加するのに必要なパラメータを設定します。

ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPsec 共有秘密情報を確立することによりロードバランシング クラスタを設定する。これらの値は、クラスタ内の各デバイスで同一です。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

前提条件

暗号化を使用する場合は、インターフェイス内にロード バランシングを設定する必要があります。そのインターフェイスがロード バランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

手順の詳細

ロード バランシングを実装するには、次の手順を実行して、同じプライベート LAN-to-LAN ネットワーク上の 2 つ以上のデバイスを、論理的に仮想クラスタとしてグループ化します。

ステップ 1　[Wizards] > [High Availability and Scalability] を選択します。

ステップ 2　[Configuration Type] 画面で、[Configure VPN Cluster Load Balancing] をクリックしてから、[Next] をクリックします。

ステップ 3　仮想クラスタ全体を表す 1 つの IP アドレスを選択します。仮想クラスタ内のすべての ASA が共有するパブリック サブネットのアドレス範囲内で、IP アドレスを指定します。

ステップ 4　このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロード バランシングに使用する UDP の宛先ポート番号を入力します。

ステップ 5　IPsec 暗号化をイネーブルにして、デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにするには、[Enable IPsec Encryption] チェックボックスをオンにします。共有秘密を指定し、確認する必要があります。仮想クラスタ内の ASA は、IPsec を使用する LAN-to-LAN トンネルを介して通信します。IPsec 暗号化をディセーブルにするには、[Enable IPsec Encryption] チェックボックスをオフにします。

ステップ 6　IPsec 暗号化をイネーブルにするときに、IPsec ピア間の共有秘密を指定します。入力した値は、連続するアスタリスク文字として表示されます。

ステップ 7　クラスタ内のこのデバイスに割り当てるプライオリティを指定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。プライオリティを高く設定すると（たとえば 10）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

（注）　仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタ マスターの役割を果たすと想定されます。どの仮想クラスタにもマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、セカンダリ デバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタ マスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

ステップ 8　このデバイスのパブリック インターフェイスの名前または IP アドレスを指定します。

ステップ 9　このデバイスのプライベート インターフェイスの名前または IP アドレスを指定します。

ステップ 10　VPN クライアント接続をクラスタ デバイスにリダイレクトするとき、外部 IP アドレスの代わりにクラスタ デバイスのホスト名とドメイン名を使用して、VPN クラスタ マスターによって完全修飾ドメイン名が送信されるようにするには、[Send FQDN to client instead of an IP address when redirecting] チェックボックスをオンにします。

ステップ 11　[Next] をクリックします。[Summary] 画面でコンフィギュレーションを確認します。

ステップ 12　[Finish] をクリックします。

VPN クラスタ ロード バランシングの設定が ASA に送信されます。

ロード バランシングの設定（ウィザードを使用しない場合）

[Load Balancing]ペイン（[Configuration] > [Remote Access VPN] > [Load Balancing]）では、ASA のロード バランシングをイネーブルにすることができます。ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPsec 共有秘密情報を確立することによりロードバランシング クラスタを設定する。これらの値は、クラスタ内のすべてのデバイスで同一です。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

前提条件

- 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。
- 暗号化を使用する場合は、インターフェイス内にロード バランシングを設定する必要があります。そのインターフェイスがロード バランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

ステップ 1　[Configuration] > [Remote Access VPN] > [Load Balancing] の順に選択します。

ステップ 2　[Participate in Load Balancing] をオンにして、この ASA がロードバランシング クラスタに参加していることを指定します。

ロード バランシングに参加するすべての ASA に対してこの方法でロード バランシングをイネーブルにする必要があります。

ステップ 3　[VPN Cluster Configuration] エリアで、次のフィールドを設定します。これらの値は、仮想クラスタ全体で同じである必要があります。すべてのクラスタに同一のクラスタ設定を行う必要があります。

- [Cluster IPv4 Address]：IPv4 仮想クラスタ全体を表す単一の IPv4 アドレスを指定します。仮想クラスタ内のすべての ASA が共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。
  - [UDP Port]：このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロードバランシングに使用する UDP の宛先ポート番号を入力します。
- [Cluster IPv6 Address]：IPv6 仮想クラスタ全体を表す単一の IPv6 アドレスを指定します。仮想クラスタ内のすべての ASA が共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。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。

（注）　少なくとも 1 台の DNS サーバに DNS サーバ グループが設定されており、ASA インターフェイスの 1 つで DNS ルックアップがイネーブルにされている場合、[Cluster IPv4 Address] および [Cluster IPv6 Address] フィールドでは、仮想クラスタの完全修飾ドメイン名も指定できます。

- [Enable IPSec Encryption]：IPSec 暗号化をイネーブルまたはディセーブルにします。このボックスをオンにして、共有秘密情報を指定して確認します。仮想クラスタ内の ASA は、IPsec を使用する LAN-to-LAN トンネルを介して通信します。デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにするには、このチェックボックスをオンにします。
- [IPSec Shared Secret]：IPSec 暗号化がイネーブルになっているときに、IPSec ピア間の共有秘密情報を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。
- [Verify Secret]：共有秘密情報を再入力します。[IPSec Shared Secret] ボックスに入力された共有秘密情報の値を確認します。

ステップ 4　特定の ASA の [VPN Server Configuration] エリアのフィールドを設定します。

- [Public Interface]：このデバイスのパブリック インターフェイスの名前または IP アドレスを指定します。
- [Private Interface]：このデバイスのプライベート インターフェイスの名前または IP アドレスを指定します。
- [Priority]：クラスタ内でこのデバイスに割り当てるプライオリティを指定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。優先順位を高く設定すれば（10 など）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

（注）　仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタ マスターの役割を果たすと想定されます。仮想クラスタにはマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、バックアップ デバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタ マスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

- [NAT Assigned IPv4 Address]：このデバイスの IP アドレスを NAT によって変換した結果の IP アドレスを指定します。NAT を使用しない場合（またはデバイスが NAT を使用するファイアウォールの背後にはない場合）は、このフィールドを空白のままにしてください。
- [NAT Assigned IPv6 Address]：このデバイスの IP アドレスを NAT によって変換した結果の IP アドレスを指定します。NAT を使用しない場合（またはデバイスが NAT を使用するファイアウォールの背後にはない場合）は、このフィールドを空白のままにしてください。
- [Send FQDN to client]：このチェックボックスをオンにすると、VPN クラスタ マスターが VPN クライアント接続をクラスタ デバイスにリダイレクトするときに、外部 IP アドレスの代わりにクラスタ デバイスのホスト名とドメイン名を使用して完全修飾ドメイン名が送信されるようになります。

  デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、その証明書はバックアップ デバイスにリダイレクトされたときに無効になります。

  VPN クラスタ マスターとして、ASA は、VPN クライアント接続を別のクラスタ デバイスにリダイレクトする場合に、DNS 逆ルックアップを使用して、そのクラスタ デバイス（クラスタ内の別の ASA）の外部 IP アドレスではなく完全修飾ドメイン名（FQDN）を送信できます。

  クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

（注）　IPv6 を使用し、FQDNS をクライアントに送信するときに、これらの名前は DNS を通じて ASA で解決できる必要があります。

FQDN を使用したクライアントレス SSL VPN ロード バランシングのイネーブル化

ステップ 1　[Send FQDN to client instead of an IP address when redirecting] チェックボックスをオンにして、ロード バランシングでの FQDN の使用をイネーブルにします。

ステップ 2　使用する ASA の外部インターフェイスのエントリがまだ存在しない場合は、各インターフェイスのエントリを DNS サーバに追加します。ASA の各外部 IP アドレスには、ルックアップ用に関連付けられている DNS エントリが含まれている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。

ステップ 3　[Configuration] > [Device Management] > [DNS] > [DNS Client] ダイアログボックスで、DNS サーバへのルートを持つインターフェイスの ASA での DNS ルックアップをイネーブルにします。

ステップ 4　ASA で DNS サーバの IP アドレスを定義します。これには、このダイアログボックスの [Add] をクリックします。[Add DNS Server Group] ダイアログボックスが開きます。追加する DNS サーバの IPv4 または IPv6 アドレスを入力します。たとえば、192.168.1.1 または 2001:DB8:2000::1 です。

ステップ 5　[OK] および [Apply] をクリックします。

グローバル NAC パラメータの設定

ASA は、Extensible Authentication Protocol（EAP）over UDP（EAPoUDP）のメッセージを使用して、リモート ホストのポスチャを確認します。ポスチャ検証は、リモート ホストにネットワーク アクセス ポリシーを割り当てる前に、そのホストがセキュリティの必要条件を満たしているかどうかを調べることです。ASA でネットワーク アドミッション コントロールを設定する前に、NAC 用に Access Control Server を設定しておく必要があります。

フィールド

[NAC] ペインでは、すべての NAC 通信に適用される属性を設定できます。ペインの一番上に表示される次のグローバル属性は、ASA とリモート ホストの間の EAPoUDP メッセージングに適用されます。

- [Port]：ホストの Cisco Trust Agent（CTA）との EAP over UDP 通信で使用するポート番号。この番号は、CTA で設定されているポート番号と一致する必要があります。値は 1024 ～ 65535 の範囲で入力します。デフォルト設定は 21862 です。
- [Retry if no response]：ASA が EAP over UDP メッセージを再送信する回数。この属性により、Rechallenge Interval の期限切れに対して送信されるメッセージの連続再試行回数を制限します。この設定は秒単位です。値は 1 ～ 3 の範囲で入力します。デフォルト設定は 3 です。
- [Rechallenge Interval]：ASA は、EAPoUDP メッセージをホストに送信するときにこのタイマーを開始します。ホストからの応答があるとタイマーがクリアされます。応答を受信する前にタイマーが期限切れになると、ASA はメッセージを再送信します。この設定は秒単位です。1 ～ 60 の範囲で値を入力します。デフォルト設定は 3 です。
- [Wait before new PV Session]：ASA は、リモート ホストの NAC セッションを保持状態にしたときにこのタイマーを開始します。セッションが保持状態になるのは、送信された EAPoUDP メッセージの数が [Retry if no response] 設定の値に達しても応答を受信できない場合です。ASA は、ACS サーバから「Access Reject」メッセージを受信した後にも、このタイマーを開始します。タイマーが期限切れになると、ASA はリモート ホストとの新しい EAP over UDP アソシエーションの開始を試みます。この設定は秒単位です。60 ～ 86400 の範囲で値を入力します。デフォルト設定は 180 です。

[NAC] ペインの [Clientless Authentication] 領域では、EAPoUDP 要求に応答しないホストの設定値を設定できます。CTA が実行されていないホストは、これらの要求に応答しません。

- [Enable clientless authentication]：クライアントレス認証をイネーブルにします。ASA は、ユーザ認証要求の形式で、設定されているクライアントレス ユーザ名とパスワードを Access Control Server に送信します。次に、ACS はクライアントレス ホストのアクセス ポリシーを要求します。この属性をブランクのままにすると、ASA はクライアントレス ホストのデフォルト ACL を適用します。

- [Clientless Username]：ACS のクライアントレス ホストに設定するユーザ名。デフォルト設定は clientless です。1 ～ 64 文字の ASCII 文字を入力します。先頭および末尾のスペース、ポンド記号（#）、疑問符（?）、一重または二重引用符（' と "）、アスタリスク（*）、山カッコ（< と >）は除外します。
- [Password]：ACS のクライアントレス ホストに設定するパスワード。デフォルト設定は clientless です。4 ～ 32 文字の ASCII 文字を入力します。
- [Confirm Password]：確認のために再入力する、ACS のクライアントレス ホストに設定するパスワード。
- [Enable Audit]：クライアントがポスチャ検証要求に応答しない場合に、クライアントの IP アドレスをオプションの監査サーバに渡します。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。
- [None]：クライアントレス認証と監査サービスをディセーブルにします。

ネットワーク アドミッション コントロールのポリシーの設定

[NAC Policies] テーブルには、ASA で設定されているネットワーク アドミッション コントロール（NAC）のポリシーが表示されます。

NAC ポリシーを追加、変更、または削除するには、次のいずれかの操作を実行します。

- NAC ポリシーを追加するには、[Add] を選択します。[Add NAC Framework Policy] ダイアログボックスが開きます。
- NAC ポリシーを変更するには、そのポリシーをダブルクリックするか、ポリシーを選択して [Edit] をクリックします。[Edit NAC Framework Policy] ダイアログボックスが開きます。
- NAC ポリシーを削除するには、ポリシーを選択して [Delete] をクリックします。

次の各項では、NAC、NAC の要件、およびポリシー属性への値の割り当て方法を説明します。

NAC について

NAC では、ネットワークへのアクセスの条件としてエンドポイントの準拠性チェックと脆弱性チェックを実行することにより、ワーム、ウイルス、および不正アプリケーションによる侵入および感染からエンタープライズのネットワークを保護します。これらのチェックは、*ポスチャ検証* と呼ばれます。イントラネット上の脆弱なホストにアクセスする前に、ポスチャ検証を設定して、AnyConnect またはクライアントレス SSL VPN セッションを使用するホスト上のアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入防御ソフトウェアが最新の状態であることを確認できます。ポスチャ検証の一部として、リモート ホストで実行されているアプリケーションが最新のパッチで更新されているか検証することもできます。NAC は、ユーザ認証およびトンネルの設定の完了後に行われます。自動ネットワーク ポリシー実施が適用されないホスト（ホーム PC など）からエンタープライズ ネットワークを保護する場合は、NAC が特に有用です。

エンドポイントと ASA 間でトンネルを確立すると、ポスチャ検証がトリガーされます。

クライアントがポスチャ検証の要求に応答しない場合は、ASA を設定して、そのクライアントの IP アドレスをオプションの監査サーバに渡すことができます。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。

ポスチャ検証が成功する、またはリモート ホストが正常であることを示すトークンを受信すると、ポスチャ検証サーバは、トンネル上のトラフィックに対するアプリケーション用のネットワーク アクセス ポリシーを ASA に送信します。

ASA を含む *NAC Framework* のコンフィギュレーションには、クライアントで実行されている Cisco Trust Agent だけがポスチャ エージェントの役割を果たすことができ、Cisco Access Control Server（ACS）だけがポスチャ検証サーバの役割を果たすことができます。ACS はダイナミック ACL を使用して、各クライアントのアクセス ポリシーを決定します。

RADIUS サーバである ACS は、ポスチャ検証サーバとしての役割を果たすことに加え、トンネルの確立に必要なログイン クレデンシャルを認証できます。

（注） ASA に設定されている NAC Framework ポリシーだけが、監査サーバの使用をサポートしています。

ACS はそのポスチャ検証サーバとしての役割において、アクセス コントロール リストを使用します。ポスチャ検証が成功し、ACS によって、ASA に送信するアクセス ポリシーの一部としてリダイレクト URL が指定されると、ASA は、リモート ホストからのすべての HTTP 要求と HTTPS 要求をリダイレクト URL にリダイレクトします。ポスチャ検証サーバによってアクセス ポリシーが ASA にアップロードされると、関連するすべてのトラフィックはその宛先に到達するためにセキュリティ アプライアンスと ACS（またはその逆も同じ）の両方を通過する必要があります。

NAC フレームワーク ポリシーがグループ ポリシーに割り当てられている場合は、リモート ホストと ASA の間にトンネルが確立されるとポスチャ検証が実行されます。ただし、NAC Framework ポリシーでは、ポスチャ検証を免除されているオペレーティング システムを特定し、そのようなトラフィックをフィルタリングするためにオプションの ACL を指定できます。

使用方法、要件、および制限

NAC をサポートするように設定すると、ASA は、Cisco Secure Access Control Server のクライアントとして機能します。そのため、NAC 認証サービスを提供するために、ネットワーク上に少なくとも 1 台の Access Control Server をインストールする必要があります。

ネットワークで 1 台以上の Access Control Server を設定した後は、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add or Edit External] メニュー オプションを使用して Access Control Server グループを登録する必要があります。その後、NAC ポリシーを追加します。

ASA による NAC フレームワークのサポートは、リモート アクセス IPSec セッションとクライアントレス SSL VPN セッションに限られています。NAC Framework コンフィギュレーションは、シングル モードだけをサポートしています。

ASA における NAC では、レイヤ 3（非 VPN）および IPv6 トラフィックはサポートされていません。

フィールド

- [Policy Name]：新しい NAC ポリシーの名前を最大 64 文字で入力します。

  NAC ポリシーのコンフィギュレーションに続いて、Network (Client) Access グループ ポリシーの NAC Policy 属性の隣にポリシー名が表示されます。属性または目的を、設定する他の属性または目的と区別できるように名前を割り当てます。

- [Status Query Period]：ASA は、ポスチャ検証とステータス クエリーの応答が成功するたびに、このタイマーを開始します。このタイマーが切れると、ホスト ポスチャの変化を調べるクエリー（*ステータス クエリー*と呼ばれる）がトリガーされます。30 ～ 1800 の範囲で秒数を入力します。デフォルトの設定は 300 秒です。

- [Revalidation Period]：ASA は、ポスチャ検証が成功するたびに、このタイマーを開始します。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。ASA では、再検証中はポスチャ検証が維持されます。ポスチャ検証または再検証中にアクセス コントロール サーバが使用できない場合、デフォルトのグループ ポリシーが有効になります。ポスチャを検証する間隔を秒数で入力します。指定できる範囲は 300 ～ 86400 です。デフォルトの設定は 36000 秒です。

- [Default ACL]：（オプション）ポスチャ検証が失敗した場合、ASA は、選択された ACL に関連付けられているセキュリティ ポリシーを適用します。[None] を選択するか、リストの拡張 ACL を選択します。デフォルト設定は [None] です。設定が [None] のときにポスチャ検証に失敗した場合、ASA はデフォルト グループ ポリシーを適用します。

  [Manage] ボタンを使用して、ドロップダウン リストを読み込み、リストに ACL の設定を表示します。

- [Manage]：[ACL Manager] ダイアログボックスを開きます。クリックして、標準 ACL および各 ACL の ACE を表示、イネーブル化、ディセーブル化、削除します。[Default ACL] 属性の横のリストに [ACL] が表示されます。

- [Authentication Server Group]：ポスチャ検証用に使用する認証サーバ グループを指定します。この属性の横にあるドロップダウン リストには、ASA に設定され、リモート アクセス トンネルで利用できる RADIUS タイプのすべてのサーバ グループ名が表示されます。NAC をサポートするように設定された、少なくとも 1 台のサーバで構成される ACS グループを選択します。

- [Posture Validation Exception List] : ポスチャ検証からリモート コンピュータを除外する 1 つ以上の属性が表示されます。各エントリには、少なくともオペレーティング システムと、[Yes] または [No] いずれかの [Enabled] 設定が含まれています。オプションのフィルタが、リモート コンピュータの追加属性を一致させる ACL を識別します。ポスチャ検証からリモート コンピュータを除外するには、オペレーティング システムで構成されたエントリとフィルタの両方に一致する必要があります。ASA は、[Enabled] 設定が [No] に設定されているエントリを無視します。

- [Add]：エントリを [Posture Validation Exception] リストに追加します。
- [Edit]：[Posture Validation Exception] リストのエントリを修正します。
- [Delete]：エントリを [Posture Validation Exception] リストから削除します。

次の作業

NAC ポリシーのコンフィギュレーションに続いて、そのポリシーをアクティブにするためにグループ ポリシーに割り当てる必要があります。このようにするには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [General] > [More Options] を選択し、[NAC Policy] 属性の横にあるドロップダウン リストから NAC ポリシー名を選択します。

[Add/Edit Posture Validation Exception]

[Add/Edit Posture Validation Exception] ダイアログ ペインでは、オペレーティング システム、およびフィルタに一致するオプションの属性に基づいてリモート コンピュータをポスチャ検証から除外できます。

- [Operating System]：リモート コンピュータのオペレーティング システムを選択します。コンピュータでこのオペレーティング システムが実行されている場合は、ポスチャ検証から除外されます。デフォルト設定は空白です。
- [Enable]：[Enabled] をオンにした場合にだけ、ASA は、このペインに表示される属性設定がリモート コンピュータに存在するかどうかをチェックします。オフにした場合は、属性設定が無視されます。デフォルト設定では、無効になっています。
- [Filter]（オプション）：コンピュータのオペレーティング システムが Operating System 属性の値に一致する場合に、トラフィックに ACL を適用してフィルタリングします。
- [Manage]：[ACL Manager] ダイアログボックスを開きます。クリックして、標準 ACL および各 ACL の ACE を表示、イネーブル化、ディセーブル化、削除します。[Default ACL] 属性の横のリストに [ACL] が表示されます。このボタンを使用して、[Filter] 属性の横のリストに入力します。

CHAPTER 3

一般的な VPN 設定

AnyConnect Customization/Localization

AnyConnect VPN クライアントをカスタマイズして、リモート ユーザに自社企業のイメージを表示することができます。Windows、Linux、および Mac OS X コンピュータ上で稼働するクライアントがあります。[AnyConnect Customization/Localization] の次の ASDM 画面では、以下のタイプのカスタマイズされたファイルをインポートできます。

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

各ダイアログでは次のアクションを実行できます。

- [Import] をクリックすると、[Import AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。
- [Export] をクリックすると、[Export AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。
- [Delete] をクリックすると、選択したオブジェクトが削除されます。

制約事項

- Windows Mobile デバイスで稼働する AnyConnect クライアントのカスタマイズはサポートされていません。

[AnyConnect Customization/Localization] > [Resources]

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

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

[AnyConnect Customization/Localization] > [Binary] および [Script]

ES - The samelink is used in ASDM for both Binary and Script, so share this link for now, and submit a defect against ASDM to have them add another link.

[AnyConnect Customization/Localization] > [Binary]

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

[Import] ダイアログのフィールドは次のとおりです。

- [Name]：置き換える AnyConnect ファイルの名前を入力します。
- [Platform]：ファイルを実行する OS プラットフォームを選択します。
- [Select a file]：ファイル名は、インポートするファイルの名前と同じである必要はありません。

[AnyConnect Customization/Localization] > [Script]

スクリプトの展開とスクリプトの制限事項の詳細については、『*AnyConnect VPN Client Administrators Guide*』を参照してください。

[Import] ダイアログのフィールドは次のとおりです。

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

  AnyConnect によって、ASA で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、ASA は、リモート コンピュータ上の適切なターゲット ディレクトリにスクリプトをダウンロードし、*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、ASA 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。

  スクリプトの実行の信頼性を確保するために、すべての ASA で同じスクリプトを展開するように設定します。スクリプトを修正または置換する場合は、旧バージョンと同じ名前を使用し、ユーザが接続する可能性のあるすべての ASA に置換スクリプトを割り当てます。ユーザが接続すると、新しいスクリプトにより同じ名前のスクリプトが上書きされます。
- [Platform]：ファイルを実行する OS プラットフォームを選択します。
- [Select a file]：ファイル名は、スクリプトに対して指定した名前と同じである必要はありません。

  ASDM によってファイルがソース ファイルからインポートされ、ステップ 3 で [Name] に対して指定した新しい名前が作成されます。

[AnyConnect Customization/Localization] > [GUI Text and Messages]

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

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

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

変換テーブルのメッセージをカスタマイズする場合、msgid は変更せずに、msgstr のテキストを変更してください。

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

[Template] セクション

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

[AnyConnect Customization/Localization] > [Customized Installer Transforms]

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

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

[AnyConnect Customization/Localization] > [Localized Installer Transforms]

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

IPsec VPN クライアント ソフトウェア

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

クライアント ソフトウェアの場所の編集

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

グループ ポリシー

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

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

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

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

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

これらのパラメータを設定する前に、次の項目を設定する必要があります。

- アクセス時間（[General]> [More Options] > [Access Hours]）。
- フィルタ（[General]> [More Options] > [Filters]）。
- フィルタリングおよびスプリット トンネリング用のネットワーク リスト（[Configuration]> [Policy Management] > [Traffic Management] > [Network Lists]）。
- ユーザ認証サーバと内部認証サーバ（[Configuration]> [System] > [Servers] > [Authentication]）。

次のタイプのグループ ポリシーを設定できます。

- 「外部グループ ポリシーの設定」：外部グループ ポリシーは、ASA から RADIUS または LDAP サーバを指して、ほとんどのポリシー情報を取得します。それ以外の情報は、内部グループ ポリシーに設定されます。外部グループ ポリシーは、ネットワーク（クライアント）アクセス VPN 接続、クライアントレス SSL VPN 接続、およびサイト間 VPN 接続に対して同じ方法で設定されます。
- 「ネットワーク（クライアント）アクセス内部グループ ポリシーの設定」：これらの接続は、エンドポイントにインストールされた VPN クライアントによって開始されます。AnyConnect セキュア モビリティ クライアントおよび Cisco IPsec VPN クライアントは、VPN クライアントの使用例です。VPN クライアントが認証されると、オンサイトの場合、リモート ユーザは企業ネットワークまたはアプリケーションにアクセスできます。リモート ユーザと企業ネットワーク間のデータ トラフィックは、暗号化によってインターネットを通過する際に保護されます。
- 「クライアントレス SSL VPN 内部グループ ポリシーの設定」：これは、ブラウザ ベースの VPN アクセスとも呼ばれます。ASA のポータル ページに正常にログインすると、リモート ユーザは Web ページに表示されるリンクから企業ネットワークとアプリケーションにアクセスできます。リモート ユーザと企業ネットワーク間のデータ トラフィックは、SSL トンネルを通過する際に保護されます。
- 「サイト間内部グループ ポリシーの設定」

[Group Policy] ペイン フィールド

現在設定されているグループ ポリシーと、VPN グループ ポリシーを管理するための [Add]、[Edit]、および [Delete] ボタンが表示されます。

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

外部グループ ポリシーの設定

外部グループ ポリシーは、外部サーバから認可および認証の属性値を取得します。このグループ ポリシーでは、ASA が属性のクエリーを実行できる RADIUS または LDAP サーバ グループを特定し、その属性を取得するときに使用するパスワードを指定します。

ASA の外部グループ名は、RADIUS サーバのユーザ名を参照しています。つまり、ASA に外部グループ X を設定する場合、RADIUS サーバはクエリーをユーザ X に対する認証要求と見なします。そのため、外部グループは実際には、ASA にとって特別な意味を持つ、RADIUS サーバ上のユーザ アカウントということになります。外部グループ属性が認証する予定のユーザと同じ RADIUS サーバに存在する場合、それらの間で名前を重複させることはできません。

外部サーバを使用するように ASA を設定する前に、正しい ASA 認可属性でサーバを設定し、それらの属性のサブセットから個々のユーザに対する個別の許可を割り当てる必要があります。外部サーバを設定するには、「認可および認証用の外部サーバ」の説明に従ってください。

外部グループ ポリシーのフィールド

- [Name]：追加または変更するグループ ポリシーを特定します。[Edit External Group Policy] の場合、このフィールドは表示専用です。
- [Server Group]：このポリシーの適用先として利用できるサーバ グループを一覧表示します。

- [New]：新しい RADIUS サーバ グループまたは新しい LDAP サーバ グループを作成するかどうかを選択できるダイアログボックスを開きます。どちらの場合も [Add AAA Server Group] ダイアログボックスが開きます。
- [Password]：このサーバ グループ ポリシーのパスワードを指定します。

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

AAA サーバでのパスワード管理

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

（注） 現在のところ MS-CHAP をサポートしていても、MS-CHAPv2 はサポートしていない RADIUS サーバもあります。この機能では MS-CHAPv2 が必要になるので、この点についてベンダーにお問い合わせください。

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

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

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

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

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

AnyConnect でのパスワードのサポート

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

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

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

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

ASA は、次の条件下ではパスワード管理をサポートしません。

- ローカル（内部）認証を使用する場合
- LDAP 認証を使用する場合
- RADIUS 認証のみを使用するときに、ユーザが RADIUS サーバ データベースに存在する場合

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

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

ネットワーク（クライアント）アクセス内部グループ ポリシーの設定

内部グループ ポリシーの一般属性の設定

[Add or Edit Group Policy] ダイアログボックスでは、追加または編集するグループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

ASDM を起動し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add or Edit Internal Group Policy] > [General] を選択して、内部グループ ポリシーの一般属性を設定できます。

フィールド

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

- [Name]：このグループ ポリシーの名前を最大 64 文字で指定します（スペースの使用可）。Edit 機能の場合、このフィールドは読み取り専用です。
- [Banner]：ログイン時にユーザに対して表示するバナー テキストを指定します。長さは最大 491 文字です。デフォルト値はありません。

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

  - IPsec クライアント ユーザの場合は、/n タグを使用します。
  - AnyConnect クライアント ユーザの場合は、
 タグを使用します。
- [SCEP forwarding URL]：クライアント プロファイルで SCEP プロキシを設定する場合に必要な CA のアドレス。

- [Address Pools]：このグループ ポリシーで使用する 1 つ以上の IPv4 アドレス プールの名前を指定します。[Inherit] チェックボックスがオンの場合、グループ ポリシーはデフォルト グループ ポリシーで指定されている IPv4 アドレス プールを使用します。IPv4 アドレス プールを追加または編集する方法の詳細については「ローカル IP アドレス プールの設定」（P.4-3）を参照してください。

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

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

  [Select]：[Inherit] チェックボックスをオフにして、[Select] コマンド ボタンをアクティブにします。[Select] をクリックすると、前述のような [Select Address Pools] ダイアログボックスが開きます。IPv6 アドレス プールを追加または編集する方法の詳細については「ローカル IP アドレス プールの設定」（P.4-3）を参照してください。

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

- [More Options]：フィールドの右側にある下矢印をクリックして、このグループ ポリシーの追加の設定可能なオプションを表示します。
- [Tunneling Protocols]：このグループが使用できるトンネリング プロトコルを指定します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。
  - [Clientless SSL VPN]：SSL/TLS による VPN の使用法を指定します。この VPN では、ソフトウェアやハードウェアのクライアントを必要とせずに、Web ブラウザを使用して ASA へのセキュアなリモートアクセス トンネルを確立します。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
  - [SSL VPN Client]：Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアントの使用を指定します。AnyConnect クライアントを使用している場合は、このプロトコルを選択して Mobile User Security（MUS）がサポートされるようにする必要があります。
  - [IPsec IKEv1]：IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
  - [IPsec IKEv2]：AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェア アップデート、クライアント プロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
  - [L2TP over IPsec]：多くの PC およびモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザが、パブリック IP ネットワークを介してセキュリティ アプライアンス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。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。セキュリティ アプライアンスは、IPsec 転送モード用に設定する必要があります。

- [Filter]：IPv4 または IPv6 接続で使用するアクセス コントロール リストを指定するか、グループ ポリシーから値を継承するかどうかを指定します。フィルタは、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、[Manage] をクリックします。
- [NAC Policy]：このグループ ポリシーに適用するネットワーク アドミッション コントロール ポリシーの名前を選択します。オプションの NAC ポリシーを各グループ ポリシーに割り当てることができます。デフォルト値は --None-- です。
- [Manage]：[Configure NAC Policy] ダイアログボックスが開きます。1 つ以上の NAC ポリシーを設定すると、[NAC Policy] 属性の横のドロップダウン リストに、設定した NAC ポリシー名がオプションとして表示されます。
- [Access Hours]：このユーザに適用される既存のアクセス時間ポリシーがある場合はその名前を選択するか、または新しいアクセス時間ポリシーを作成します。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [--Unrestricted--] です。[Manage] をクリックして、[Browse Time Range] ダイアログボックスを開きます。このダイアログボックスでは、時間範囲を追加、編集、または削除できます。
- [Simultaneous Logins]：このユーザに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザ アクセスを禁止します。

  （注）　最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

- [Restrict Access to VLAN]：（オプション）「VLAN マッピング」とも呼ばれます。このパラメータにより、このグループ ポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。ASA は、このグループから選択した VLAN にすべてのトラフィックを転送します。この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。ドロップダウン リストには、デフォルト値（Unrestricted）の他に、この ASA で設定されている VLAN だけが表示されます。

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

- [Connection Profile (Tunnel Group) Lock]：このパラメータを使用すると、選択された接続プロファイル（トンネル グループ）を使用する VPN アクセスのみを許可し、別の接続ファイルを使用するアクセスを回避できます。デフォルトの継承値は [None] です。
- [Maximum Connect Time]：[Inherit] チェックボックスがオフである場合、このパラメータは、ユーザの最大接続時間を分単位で指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分で、最長時間は 35791394 分（4000 年超、その可能性はほとんどありません）です。接続時間を無制限にするには、[Unlimited] をオンにします（デフォルト）。
- [Idle Timeout]：[Inherit] チェックボックスがオフである場合、このパラメータは、ユーザのアイドル タイムアウト時間を分単位で指定します。この期間、ユーザ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。デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。この値は、クライアントレス SSL VPN のユーザには適用されません。
- [Security Group Tag (SGT)]：このグループ ポリシーに接続する VPN ユーザに割り当てられる SGT タグの数値を入力します。

- [On smart card removal]：デフォルト オプション [Disconnect] で、認証に使用されるスマート カードが取り外されると、クライアントは接続を切断します。接続の間、スマート カードをコンピュータに保持することをユーザに要求しない場合は、[Keep the connection] をクリックします。

  スマート カードの取り外しに関する設定は、RSA スマート カードを使用する Microsoft Windows でのみ機能します。

内部グループ ポリシーのサーバ属性の設定

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

（注） ここで行った変更は、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　[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。

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

AnyConnect 3.0.4 以降の場合、[DNS Servers] フィールドで最大 25 台の DNS サーバ エントリをサポートし、それ以前のリリースでは、最大 10 台の DNS サーバ エントリをサポートします。

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。

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。WINS サーバはフル トンネル クライアント（IPsec、AnyConnect、SVC、L2TP/IPsec）のみに適用され、名前解決に使用されます。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（オプション）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。

AnyConnect トラフィックに対するスプリット トンネリングの設定について

スプリット トンネリングは、VPN トンネル（暗号化）と VPN トンネル外の他のネットワーク トラフィック（非暗号化、つまり「クリア テキスト」）を介して一部の AnyConnect ネットワーク トラフィックを誘導します。

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

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

アクセス リストを作成する場合：

- アクセス コントロール リストには IPv4 および IPv6 両方のアドレスを指定できます。
- 標準 ACL を使用すると、1 つのアドレスまたはネットワークのみが使用されます。
- 拡張 ACL を使用すると、ソース ネットワークがスプリット トンネリング ネットワークになります。この場合、宛先ネットワークは無視されます。
- any が設定されたアクセス リストや、split include または split exclude が 0.0.0.0/0.0.0.0 または ::/0 に設定されたアクセス リストは、クライアントに送信されません。すべてのトラフィックをトンネル経由で送信するには、スプリット トンネル ポリシーに対して [Tunnel All Networks] を選択します。
- アドレス 0.0.0.0/255.255.255.255 または ::/128 は、スプリット トンネル ポリシーが [Exclude Network List Below] の場合にのみクライアントに送信されます。この設定は、トンネル トラフィックがローカル サブネット宛でないことをクライアントに通知します。
- AnyConnect では、スプリット トンネリング ポリシーで指定されたすべてのサイト、**および** ASA によって割り当てられた IP アドレスと同じサブネット内に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 によって割り当てられた IP アドレスが 10.1.1.1、マスクが 255.0.0.0 の場合、エンドポイント デバイスは、スプリット トンネリング ポリシーに関係なく、10.0.0.0/8 を宛先とするすべてのトラフィックを渡します。そのため、割り当てられた IP アドレスが、期待されるローカル サブネットを適切に参照するように、ネットマスクを使用します。

前提条件

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

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

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。

AnyConnect トラフィックに対するスプリット トンネリングの設定

ステップ 1　ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] に移動します。

ステップ 2　[Add] をクリックして新しいグループ ポリシーを追加するか、既存のグループ ポリシーを選択して [Edit] をクリックします。

ステップ 3　[Advanced] > [Split Tunneling] を選択します。

ステップ 4　[DNS Names] フィールドに、トンネルを介して AnyConnect で解決するドメイン名を入力します。これらの名前は、プライベート ネットワーク上のホストに対応します。split-include トンネリングが設定されている場合は、指定された DNS サーバがネットワーク リストに含まれている必要があります。フィールドには、完全修飾ドメイン名、IPv4 アドレス、または IPv6 アドレスを入力できます。

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

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

ステップ 6　スプリット トンネリングを設定するには、[Inherit] チェックボックスをオフにし、スプリット トンネリング ポリシーを選択します。[Inherit] チェックボックスをオフにしない場合、グループ ポリシーでは、デフォルト 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 ポリシーのデフォルト設定は [Tunnel All Networks] です。

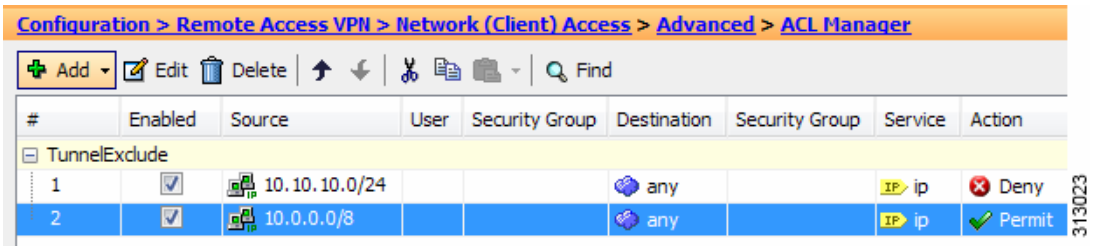
スプリット トンネリング ポリシーを定義するには、ドロップダウン [Policy] および [IPv6 Policy] から選択します。[Policy] フィールドでは、IPv4 ネットワーク トラフィックのスプリット トンネリング ポリシーを定義します。[IPv6 Policy] フィールドでは、IPv6 ネットワーク トラフィックのスプリット トンネリング ポリシーを選択します。そうした違い以外は、これらのフィールドの目的は同じです。

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

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

  次に例を示します。



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

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

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

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

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

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

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

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

ステップ 9　[OK] をクリックします。

サブネットの除外をサポートするための Linux の設定

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

ステップ 1　ASDM に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] に移動します。

ステップ 2　[Add] をクリックし、**circumvent-host-filtering** という名前のカスタム属性を作成して、その値を **true** に設定します。

ステップ 3　クライアント ファイアウォールに使用するグループ ポリシーを編集し、[Advanced] > [AnyConnect Client] > [Custom Attributes] に移動します。

ステップ 4　作成したカスタム属性 **circumvent-host-filtering** をスプリット トンネリングに使用するグループ ポリシーに追加します。

内部グループ ポリシーでのブラウザ プロキシの設定

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

このダイアログボックスでは、Microsoft Internet Explorer の属性を設定します。

[Browser Proxy] のフィールド

- [Proxy Server Policy]：クライアント PC の Microsoft Internet Explorer ブラウザのプロキシ アクション（「メソッド」）を設定します。

  - [Do not modify client proxy settings]：このクライアント PC の Internet Explorer の HTTP ブラウザ プロキシ サーバ設定を変更しません。
  - [Do not use proxy]：クライアント PC の Internet Explorer の HTTP プロキシ設定をディセーブルにします。
  - [Select proxy server settings from the following]：選択内容に応じて、[Auto detect proxy]、[Use proxy server settings given below]、および [Use proxy auto configuration (PAC) given below] のチェックボックスをオンにします。
  - [Auto-detect proxy]：クライアント PC で、Internet Explorer の自動プロキシ サーバ検出の使用をイネーブルにします。
  - [Use proxy server settings specified below]：[Proxy Server Name or IP Address] フィールドで設定された値を使用するように、Internet Explorer の HTTP プロキシ サーバ設定値を設定します。
  - [Use proxy auto configuration (PAC) given below]：[Proxy Auto Configuration (PAC)] フィールドで指定したファイルを、自動コンフィギュレーション属性のソースとして使用するように指定します。

- [Proxy Server Settings]：Microsoft Internet Explorer を使用して、Microsoft クライアントのプロキシ サーバ パラメータを設定します。
  - [Server Address and Port]：このクライアント PC で適用される、Microsoft Internet Explorer サーバの IP アドレスまたは名前、およびポートを指定します。
  - [Bypass Proxy Server for Local Addresses]：クライアント PC での Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定値を設定します。[Yes] を選択するとローカル バイパスがイネーブルになり、[No] を選択するとローカル バイパスがディセーブルになります。
  - [Exception List]：プロキシ サーバ アクセスから除外するサーバの名前と IP アドレスを一覧表示します。プロキシ サーバ経由のアクセスを行わないアドレスのリストを入力します。このリストは、[Internet Explorer の Proxy Settings] ダイアログボックスにある [Exceptions] リストに相当します。
- [Proxy Auto Configuration Settings] : PAC URL は自動設定ファイルの URL を指定します。このファイルには、ブラウザがプロキシ情報を探せる場所が記述されています。プロキシ自動コンフィギュレーション（PAC）機能を使用する場合、リモート ユーザは、Cisco AnyConnect VPN クライアントを使用する必要があります。

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

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

次に、PAC ファイルを使用する例をいくつか示します。

- ロード バランシングのためリストからプロキシをランダムに選択します。
- サーバのメンテナンス スケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
- プライマリ プロキシで障害が発生した場合に備えて、使用するバックアップ プロキシ サーバを指定します。
- ローカル サブネットを元に、ローミング ユーザ用に最も近いプロキシを指定します。

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

- Proxy Lockdown
  - [Allow Proxy Lockdown for Client System] : この機能をイネーブルにすると、AnyConnect VPN セッションの間、Microsoft Internet Explorer の [接続] タブが非表示になります。この機能をディセーブルにすると、[接続] タブの表示は変更されません。このタブのデフォルト設定は、ユーザのレジストリ設定に応じて表示または非表示になります。

内部グループ ポリシーの詳細な AnyConnect クライアント属性の設定

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] には、このグループ ポリシーで設定可能な AnyConnect クライアントの属性が表示されます。

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

（注） [Keep Installer on Client System] は、AnyConnect クライアントのバージョン 2.5 以降でサポートされていません。

- [Datagram Transport Layer Security (DTLS)]：一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスを改善します。
- [DTLS Compression]：DTLS における圧縮を設定します。
- [SSL Compression]：SSL/TLS における圧縮を設定します。
- [Ignore Don't Defrag (DF) Bit]：この機能では、DF ビットが設定されているパケットを強制的にフラグメンテーションして、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバに対する使用などがあります。
- [Client Bypass Protocol]：クライアント プロトコル バイパスでは、ASA が IPv6 トラフィックだけを予期しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定します。

AnyConnect クライアントが ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。クライアント バイパス プロトコルでは、ASA が IP アドレスを割り当てなかったトラフィックをドロップするか、または ASA をバイパスしてクライアントからの暗号化なし、つまり「クリア テキスト」としての送信を許可するかを決定します。

たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコル機能がディセーブルの場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルがイネーブルの場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

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

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

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

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

- [MTU]：SSL 接続の MTU サイズを調整します。256 ～ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLS のオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。
- [Keepalive Messages] : [Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブ メッセージの間隔をイネーブルおよび調整して、プロキシ、ファイアウォール、または NAT デバイスを通した接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモート ユーザが、Microsoft Outlook や Microsoft Internet Explorer などのソケット ベースのアプリケーションを実際に実行していないときでも、クライアントが切断と再接続を行わないことが保証されます。
- [Optional Client Modules to Download]：ダウンロード時間を最小限に抑えるために、AnyConnect クライアントは、サポートする各機能で必要とされるモジュールだけを（ASA から）ダウンロードするように要求します。次のような他の機能をイネーブルにするモジュールの名前を指定する必要があります。AnyConnect クライアントのバージョン 3.0 には、次のモジュールが含まれています（旧バージョンではモジュールの数が少なくなります）。

- AnyConnect DART : トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システム ログのスナップショットおよびその他の診断情報がキャプチャされ、.zip ファイルがデスクトップに作成されます。
- AnyConnect ネットワーク アクセス マネージャ：以前は Cisco Secure Services Client と呼ばれていました。このモジュールでは、802.1X（レイヤ 2）が提供され、有線ネットワークおよびワイヤレス ネットワークへのアクセスのデバイス認証が AnyConnect 3.0 に統合されます。
- AnyConnect SBL：Start Before Logon（SBL）では、Windows のログイン ダイアログ ボックスが表示される前に AnyConnect を開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。
- AnyConnect Web セキュリティ モジュール : 以前は ScanSafe Hostscan と呼ばれていました。このモジュールは、AnyConnect 3.0 に統合されています。
- AnyConnect テレメトリ モジュール：悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティ アプライアンス（WSA）に送信します。WSA では、このデータを使用して、URL のフィルタリング ルールを改善します。

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

- AnyConnect ポスチャ モジュール：以前は Cisco Secure Desktop HostScan 機能と呼ばれていました。ポスチャ モジュールが AnyConnect 3.0 に統合され、AnyConnect で、ASA へのリモート アクセス接続を作成する前にポスチャ アセスメントのクレデンシャルを収集することができます。

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

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

  （注） 常時接続 VPN には、AnyConnect セキュア モビリティ機能をサポートする AnyConnect リリースが必要です。詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

- [Client Profiles to Download]：プロファイルは、AnyConnect クライアントで VPN、ネットワーク アクセス マネージャ、Web セキュリティ、およびテレメトリの設定に使用されるコンフィギュレーション パラメータのグループです。[Add] をクリックして [Select AnyConnect Client Profiles] ウィンドウを起動すると、グループ ポリシー用に以前に作成されたプロファイルを指定できます。

内部グループ ポリシーの AnyConnect ログイン設定の設定

内部グループ ポリシーの [Advanced] > [AnyConnect Client] > [Login Setting] ペインでは、リモート ユーザに AnyConnect クライアントのダウンロードを求めるプロンプトを表示するように、またはクライアントレス SSL VPN のポータル ページに接続を誘導するように ASA を設定できます。図 3-1 に、クライアントに表示されるプロンプトを示します。

図 3-1　AnyConnect クライアントのダウンロードに関してリモート ユーザに表示されるプロンプト

[Login Setting] のフィールド

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

内部グループ ポリシーの AnyConnect クライアント ファイアウォール属性の設定

内部グループ ポリシーの [Advanced] > [AnyConnect Client] > [Client Firewall] ペインでは、クライアントごとのパブリック ネットワークとプライベート ネットワークの動作に影響するクライアント システムのファイアウォールに送信するルールを設定できます。

ASA 9.0(1) 以降のリリースでは、クライアント ファイアウォールのアクセス コントロール リストは、IPv4 と IPv6 アドレスの両方のアクセス コントロール エントリをサポートします。

パブリック ネットワーク ルールを使用したローカル リソースへのクライアント アクセスの許可については、「クライアント ファイアウォールを使用した VPN におけるローカル デバイスのサポートの有効化」（P.3-36）を参照してください。

内部グループ ポリシーの AnyConnect クライアント キー再生成の設定

内部グループ ポリシーの [Advanced] > [AnyConnect Client] > [Key Regeneration] ペインでは、キー再生成のパラメータを設定します。

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

[Key Regeneration] のフィールド

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

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

内部グループ ポリシーの AnyConnect クライアント デッド ピア検出の設定

内部グループ ポリシーの [Advanced] > [AnyConnect Client] > [Dead Peer Detection] ペインでは、DPD を使用するタイミングを設定します。

Dead Peer Detection（DPD）により、ピアが応答してしない、接続で障害が発生している状態を、セキュリティ アプライアンス（ゲートウェイ）またはクライアントがすばやく確実に検出できるようにします。

ASA で DPD がイネーブルにされている場合、最適 MTU（OMTU）機能を使用して、クライアントが DTLS パケットを正常に渡すことができる最大エンドポイント MTU を検出します。最大 MTU までパディングされた DPD パケットを送信することによって、OMTU を実装します。ペイロードの正しいエコーをヘッドエンドから受信すると、MTU サイズが受け入れられます。受け入れられなかった場合、MTU は小さくされ、プロトコルで許可されている最小 MTU に到達するまで、繰り返しプローブが送信されます。

（注）　OMTU を使用しても、既存のトンネル DPD 機能を妨げることはありません。

制限事項

DPD は、埋め込みが許可されない標準実装に基づくため、この機能は、IPsec とは併用できません。

[Dead Peer Detection] のフィールド

- [Gateway Side Detection] : DPD がセキュリティ アプライアンス（ゲートウェイ）によって実行されるように指定するには、[Disable] チェックボックスをオフにします。セキュリティ アプライアンスが DPD を実行するときの間隔を 30 ～ 3600 秒の範囲で入力します。
- [Client Side Detection] : DPD がクライアントによって実行されるように指定するには、[Disable] チェックボックスをオフにします。クライアントが DPD を実行するときの間隔を 30 ～ 3600 秒の範囲で入力します。

内部グループ ポリシーの VPN アクセス ポータルのカスタマイズ

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

[Customization] のフィールド

- [Portal Customization]：AnyConnect クライアント/SSL VPN ポータル ページに適用するカスタマイゼーションを選択します。事前設定済みのポータル カスタマイゼーション オブジェクトを選択するか、またはデフォルト グループ ポリシーで定義されているカスタマイゼーションを受け入れることができます。デフォルトは DfltCustomization です。
  - [Manage]：[Configure GUI Customization objects] ダイアログボックスが開きます。このダイアログボックスでは、カスタマイゼーション オブジェクトの追加、編集、削除、インポート、またはエクスポートを指定できます。
- [Homepage URL (optional)]：グループ ポリシーに関連付けられたユーザのクライアントレス ポータルに表示するホーム ページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。クライアントレス ユーザには、認証の成功後すぐにこのページが表示されます。AnyConnect は、VPN 接続が正常に確立されると、この URL に対してデフォルトの Web ブラウザを起動します。

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

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

内部グループ ポリシーの AnyConnect クライアント カスタム属性について

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

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

カスタム属性は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] および [AnyConnect Custom Attribute Names] で事前に定義できます。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。

DAP でのカスタム属性の使用については、「DAP アクセスと許可ポリシー属性の設定」（P.5-25）を参照してください。

このポリシーのカスタム属性を設定するには、次の手順を実行します。

- [Add]（新しいカスタム属性の追加）：カスタム属性のタイプを選択または設定してから、名前付きの値を選択または設定します。この手順については次で説明します。
- [Edit]（設定したカスタム属性の編集）：この属性の他の名前付きの値を選択するか、値を省略します。
- [Delete]（設定したカスタム属性の削除）：このポリシーから属性を削除します。

（注）　カスタム属性は、別のグループ ポリシーにも関連付けられている場合は編集または削除できません。

グループ ポリシーへのカスタム属性の追加

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] > [Custom Attributes] に移動します。

ステップ 2　[Add] をクリックして [Create Custom Attribute] ペインを開きます。

ステップ 3　ドロップダウン リストから事前に定義された属性タイプを選択するか、次の手順を実行して属性タイプを設定します。

a. [Manage] をクリックし、[Configure Custom Attribute Types] ペインで [Add] をクリックします。

b. [Create Custom Attribute Type] ペインで、新しい属性の [Type] と [Description] を入力します。どちらのフィールドも必須項目です。

c. [OK] をクリックしてこのペインを閉じ、もう一度 [OK] をクリックして、新しく定義したカスタム属性のタイプを選択します。

ステップ 4　[Select Value] を選択します。

ステップ 5　[Select value] ドロップダウン リストから事前に定義された名前付きの値を選択するか、次の手順を実行して新しい名前付きの値を設定します。

a. [Manage] をクリックし、[Configure Custom Attributes] ペインで [Add] をクリックします。

b. [Create Custom Attribute Name] ペインで、前に選択または設定した属性タイプを選択し、新しい属性の [Name] と [Value] を入力します。どちらのフィールドも必須項目です。

値を追加するには、[Add] をクリックして値を入力し、[OK] をクリックします。値は 420 文字を超えてはなりません。値がこの長さを超える場合は、追加の値コンテンツのために複数の値を追加します。設定値は AnyConnect クライアントに送信される前に連結されます。

c. [OK] をクリックしてこのペインを閉じ、もう一度 [OK] をクリックして、この属性の新しく定義した名前付きの値を選択します。

ステップ 6　[Create Custom Attribute] ペインで [OK] をクリックします。カスタム属性のタイプと名前付きの値がリストに表示されます。

内部グループ ポリシー：IPsec（IKEv1）クライアント設定

内部グループ ポリシーの IPsec（IKEv1）クライアントの一般属性の設定

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

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

フィールド

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

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

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

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

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

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

クライアント アクセス ルールの定義

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

内部グループ ポリシーの IPsec（IKEv1）クライアントのクライアント ファイアウォールの設定

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

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

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

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

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

フィールド

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

  [Firewall Required] を選択した場合は、このグループのユーザ全員が、指定されたファイアウォールを使用する必要があります。ASA は、指定された、サポートされているファイアウォールがインストールおよび実行されていない状態で接続を試行したセッションをドロップします。この場合、ASA は、ファイアウォール設定が一致しないことを VPN クライアントに通知します。

（注） グループでファイアウォールを必須にする場合には、そのグループに Windows VPN クライアント以外のクライアントが存在しないことを確認してください。Windows VPN クライアント以外のクライアント（クライアント モードの ASA 5505 と VPN 3002 ハードウェア クライアントを含む）は接続できません。

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

- [Firewall Type]：シスコを含む複数のベンダーのファイアウォールを一覧表示します。[Custom Firewall] を選択すると、[Custom Firewall] の下のフィールドがアクティブになります。指定したファイアウォールが、使用できるファイアウォール ポリシーと相関している必要があります。設定したファイアウォールにより、サポートされるファイアウォール ポリシー オプションが決まります。
- [Custom Firewall]：カスタム ファイアウォールのベンダー ID、製品 ID、および説明を指定します。
  - [Vendor ID]：このグループ ポリシーのカスタム ファイアウォールのベンダーを指定します。
  - [Product ID]：このグループ ポリシー用に設定されるカスタム ファイアウォールの製品またはモデル名を指定します。
  - [Description]：（オプション）カスタム ファイアウォールについて説明します。
- [Firewall Policy]：カスタム ファイアウォール ポリシーのタイプと送信元を指定します。
  - [Policy defined by remote firewall (AYT)]：ファイアウォール ポリシーがリモート ファイアウォール（Are You There）によって定義されるように指定します。[Policy defined by remote firewall (AYT)] は、このグループのリモート ユーザのファイアウォールが、各自の PC に存在することを意味しています。このローカル ファイアウォールが、VPN クライアントにファイアウォール ポリシーを適用します。ASA は、指定されたファイアウォールがインストールされ、実行中である場合にだけ、このグループの VPN クライアントが接続できるようにします。指定されたファイアウォールが実行されていない場合、接続は失敗します。接続が確立すると、VPN クライアントがファイアウォールを 30 秒ごとにポーリングして、そのファイアウォールが実行されていることを確認します。ファイアウォールの実行が停止すると、VPN クライアントはセッションを終了します。
  - [Policy pushed (CPP)]：ポリシーがピアからプッシュされるように指定します。このオプションを選択する場合は、[Inbound Traffic Policy] および [Outbound Traffic Policy] リストと [Manage] ボタンがアクティブになります。ASA は、[Policy Pushed (CPP)] ドロップダウン リストで選択されたフィルタによって定義されるトラフィック管理ルールをこのグループの VPN クライアントに適用します。メニューで使用できる選択肢は、この ASA で定義されているフィルタで、デフォルト フィルタも含まれます。ASA がこれらのルールを VPN クライアントにプッシュすることに注意してください。ASA ではなく VPN クライアントから見たルールを作成し、定義する必要があります。たとえば、「in」と「out」はそれぞれ、VPN クライアントに着信するトラフィックと、VPN クライアントから発信されるトラフィックです。VPN クライアントにローカル ファイアウォールもある場合、ASA からプッシュされたポリシーは、ローカル ファイアウォールのポリシーと同時に機能します。いずれかのファイアウォールのルールでブロックされたすべてのパケットがドロップされます。
  - [Inbound Traffic Policy]：着信トラフィックに対して使用できるプッシュ ポリシーを一覧表示します。
  - [Outbound Traffic Policy]：発信トラフィックに対して使用できるプッシュ ポリシーを一覧表示します。
  - [Manage]：[ACL Manager] ダイアログボックスを表示します。このダイアログボックスで、アクセス コントロール リスト（ACL）を設定できます。

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

（注）　VPN 3002 ハードウェア クライアントは耐用年数末期で、サポートが終了しています。この設定については、ASA 9.2 のマニュアルを参照してください。

ローカル ユーザの VPN ポリシー属性の設定

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] ダイアログボックスが表示されます。

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。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、使用できるようにする VPN トンネリング プロトコルを選択します。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、このオプションはソフトウェア 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 を通じて安全なインターネット 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、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接続できるようにします。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。接続するたびに、必要に応じてクライアント アップデートが自動的に行われます。
- [IPsec IKEv1] : IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2] : AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェア アップデート、クライアント プロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- 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。

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。トンネル グループ ロックでは、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。同時ログイン設定は、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）　最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

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、[Default] チェックボックスは自動的に検査され、セッションのアラート間隔が 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（オプション）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（オプション）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　[OK] 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。

クライアントレス SSL VPN 内部グループ ポリシーの設定

内部グループ ポリシーのクライアントレス SSL VPN 一般属性の設定

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

[Add or Edit Group Policy] ダイアログボックスでは、追加または編集するグループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

フィールド

[Add Internal Group Policy] > [General] ダイアログボックスには、次の属性が表示されます。

- [Name]：このグループ ポリシーの名前を最大 64 文字で指定します（スペースの使用可）。Edit 機能の場合、このフィールドは読み取り専用です。
- [Banner]：ログイン時にユーザに対して表示するバナー テキストを指定します。長さは最大 491 文字です。デフォルト値はありません。

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

  – クライアントレス ユーザの場合は、
 タグを使用します。
- [Tunneling Protocols]：このグループが使用できるトンネリング プロトコルを指定します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。

  – [Clientless SSL VPN]：SSL/TLS による VPN の使用法を指定します。この VPN では、ソフトウェアやハードウェアのクライアントを必要とせずに、Web ブラウザを使用して ASA へのセキュアなリモートアクセス トンネルを確立します。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。

  – [SSL VPN Client]：Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアントの使用を指定します。AnyConnect クライアントを使用している場合は、このプロトコルを選択して MUS がサポートされるようにする必要があります。

  - [IPsec IKEv1]：IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
  - [IPsec IKEv2]：AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェア アップデート、クライアント プロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
  - [L2TP over IPsec]：多くの PC およびモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザが、パブリック IP ネットワークを介してセキュリティ アプライアンス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。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。セキュリティ アプライアンスは、IPsec 転送モード用に設定する必要があります。

- [Web ACL]：（Clientless SSL VPN 専用）トラフィックをフィルタリングする場合は、ドロップダウン リストからアクセス コントロール リスト（ACL）を選択します。選択する前に ACL を表示、変更、追加、または削除する場合は、リストの横にある [Manage] をクリックします。
- [Access Hours]：このユーザに適用される既存のアクセス時間ポリシーがある場合はその名前を選択するか、または新しいアクセス時間ポリシーを作成します。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [--Unrestricted--] です。時間範囲オブジェクトを表示または追加するには、リストの横にある [Manage] をクリックします。
- [Simultaneous Logins]：このユーザに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザ アクセスを禁止します。

（注）　最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

- [Restrict Access to VLAN]：（オプション）「VLAN マッピング」とも呼ばれます。このパラメータにより、このグループ ポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。ASA は、このグループのトラフィックすべてを、選択した VLAN に転送します。この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。ドロップダウン リストには、デフォルト値（Unrestricted）の他に、この ASA で設定されている VLAN だけが表示されます。

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

- [Connection Profile (Tunnel Group) Lock]：このパラメータを使用すると、選択された接続プロファイル（トンネル グループ）を使用する VPN アクセスのみを許可し、別の接続ファイルを使用するアクセスを回避できます。デフォルトの継承値は [None] です。
- [Maximum Connect Time]：[Inherit] チェックボックスがオフである場合、このパラメータは、ユーザの最大接続時間を分単位で指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分で、最長時間は 35791394 分（4000 年超）です。接続時間を無制限にするには、[Unlimited] をオンにします（デフォルト）。

- [Idle Timeout]：[Inherit] チェックボックスがオフである場合、このパラメータは、ユーザのアイドル タイムアウト時間を分単位で指定します。この期間、ユーザ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。デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。この値は、クライアントレス SSL VPN のユーザには適用されません。
- [Session Alert Interval]：[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。
- [Idle Alert Interval]：[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。

内部グループ ポリシーのクライアントレス SSL VPN アクセス ポータルの設定

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

フィールド

- [Bookmark List]：あらかじめ設定されたブックマーク リストを選択するか、または [Manage] をクリックして新しいリストを作成します。ブックマークはリンクとして表示され、ユーザはこのリンクを使用してポータル ページから移動できます。
- [URL Entry]：リモート ユーザが URL をポータル URL フィールドに直接入力できるようにする場合にイネーブルにします。
- [File Access Control]：共通インターネット ファイル システム（CIFS）ファイルの「非表示共有」の表示状態を制御します。非表示共有は、共有名の末尾のドル記号（$）で識別されます。たとえば、ドライブ C は C$ として共有されます。非表示共有では、共有フォルダは表示されず、ユーザはこれらの非表示リソースを参照またはアクセスすることを禁止されます。
  - [File Server Entry]：リモート ユーザがファイル サーバの名前を入力できるようにする場合にイネーブルにします。
  - [File Server Browsing]：リモート ユーザが使用可能なファイル サーバを参照できるようにする場合にイネーブルにします。
  - [Hidden Share Access]：共有フォルダを非表示にする場合にイネーブルにします。
- [Port Forwarding Control]：Java Applet によるクライアントレス SSL VPN 接続により、ユーザが TCP ベースのアプリケーションにアクセスできるようにします。
  - [Port Forwarding List]：このグループ ポリシーに関連付ける事前設定済み TCP アプリケーションのリストを選択します。新しいリストを作成したり、既存のリストを編集したりするには、[Manage] をクリックします。
  - [Auto Applet Download]：ユーザが初めてログインするときに実行される、Java Applet の自動インストールおよび起動をイネーブルにします。
  - [Applet Name]：[Applet] ダイアログボックスのタイトルバーの名前を、指定する名前に変更します。デフォルトの名前は [Application Access] です。

- [Smart Tunnel]：セキュリティ アプライアンスをパスウェイとして、また、ASA をプロキシ サーバとして使用するクライアントレス（ブラウザベース）SSL VPN セッションを使用して、スマート トンネルのオプションを指定します。
  - [Smart Tunnel Policy]：ネットワーク リストから選択し、いずれか 1 つのトンネル オプションを指定します（[use smart tunnel for the specified network]、[do not use smart tunnel for the specified network]、または [use tunnel for all network traffic]）。スマート トンネル ネットワークをグループ ポリシーまたはユーザ名に割り当てると、そのグループ ポリシーまたはユーザ名にセッションが関連付けられているすべてのユーザの場合にスマート トンネル アクセスがイネーブルになりますが、リストで指定されているアプリケーションへのスマート トンネル アクセスは制限されます。スマート トンネル リストを表示、追加、変更、または削除するには、[Manage] をクリックします。
  - [Smart Tunnel Application]：ドロップダウン リストから選択し、エンド ステーションにインストールされている TCP ベースのアプリケーション Winsock 2 をイントラネット上のサーバに接続します。スマート トンネル アプリケーションを表示、追加、変更、または削除するには、[Manage] をクリックします。
  - [Smart Tunnel all Applications]：すべてのアプリケーションをトンネリングするには、このチェックボックスをオンにします。ネットワーク リストから選択したり、エンド ユーザが外部アプリケーション用に起動する可能性がある実行ファイルを認識したりすることなく、すべてのアプリケーションがトンネリングされます。
  - [Auto Start]：ユーザのログイン時に、スマート トンネル アクセスを自動的に開始するには、このチェックボックスをオンにします。ユーザのログイン時にスマート トンネル アクセスを開始するこのオプションは Windows だけに適用されます。ユーザのログイン時にスマート トンネル アクセスをイネーブルにして、ユーザに手動で開始するように要求する場合はこのチェックボックスをオフにします。ユーザは、[Clientless SSL VPN Portal] ページの [Application Access] > [Start Smart Tunnels] ボタンを使用してアクセスを開始できます。
  - [Auto Sign-on Server List]：ユーザがサーバへのスマート トンネル接続を確立するときにユーザ クレデンシャルを再発行する場合、ドロップダウン リストからリスト名を選択します。各スマート トンネル自動サインオン リストのエントリは、ユーザ クレデンシャルのサブミッションを自動化するサーバを示します。スマート トンネル自動サインオン リストを表示、追加、変更、または削除するには、[Manage] ボタンをクリックします。
  - [Windows Domain Name (Optional)]：共通命名規則（domain\username）が認証に必要な場合、自動サインオン時にユーザ名に追加する Windows のドメインを指定します。たとえば、ユーザ名 qu_team の認証を行う場合、CISCO と入力して CISCO\qa_team を指定します。自動サインオン サーバ リストで関連するエントリを設定する場合、[Use Windows domain name with user name] オプションもオンにする必要があります。
- [ActiveX Relay]：クライアントレス ユーザが Microsoft Office アプリケーションをブラウザから起動できるようにします。アプリケーションは、セッションを使用して Microsoft Office ドキュメントのダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。

その他のオプション：

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

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

クライアントレス SSL VPN 内部グループ ポリシーのポータル カスタマイゼーションの設定

グループ ポリシーのカスタマイゼーションを設定するには、事前設定済みのポータル カスタマイゼーション オブジェクトを選択するか、またはデフォルト グループ ポリシーで定義されているカスタマイゼーションを受け入れます。表示する URL を設定することもできます。

クライアントレス SSL VPN アクセス接続にアクセス ポータルをカスタマイズするための手順は、ネットワーク アクセス クライアント接続と同じです。「内部グループ ポリシーの VPN アクセス ポータルのカスタマイズ」（P.3-21）を参照してください。

クライアントレス SSL VPN 内部グループ ポリシーのログイン設定の設定

このダイアログボックスでは、リモート ユーザに AnyConnect クライアントのダウンロードを求めるプロンプトを表示するように、またはクライアントレス SSL VPN のポータル ページに進むように ASA を設定できます。「内部グループ ポリシーの AnyConnect ログイン設定の設定」（P.3-20）を参照してください。

クライアントレス SSL VPN アクセスの内部グループ ポリシーのシングル サインオンおよび自動サインオン サーバの設定

シングル サインオン サーバと自動サインオン サーバを設定するには、第 15 章「クライアントレス SSL VPN ユーザ」を参照してください。

サイト間内部グループ ポリシーの設定

[Configuration] > [Site-to-Site VPN] > [Group Policies]

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

フィールド

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

- [Name]：このグループ ポリシーの名前を指定します。Edit 機能の場合、このフィールドは読み取り専用です。
- [Tunneling Protocols]：このグループが許可するトンネリング プロトコルを指定します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。

- [Clientless SSL VPN]：SSL/TLS による VPN の使用法を指定します。この VPN では、ソフトウェアやハードウェアのクライアントを必要とせずに、Web ブラウザを使用して ASA へのセキュアなリモートアクセス トンネルを確立します。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
- [SSL VPN Client]：Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアントの使用を指定します。AnyConnect クライアントを使用している場合は、このプロトコルを選択して MUS がサポートされるようにする必要があります。
- [IPsec IKEv1]：IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2]：AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェア アップデート、クライアント プロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- [L2TP over IPsec]：多くの PC およびモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザが、パブリック IP ネットワークを介してセキュリティ アプライアンス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。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。セキュリティ アプライアンスは、IPsec 転送モード用に設定する必要があります。

- [Filter]：（Network (Client) Access 専用）使用するアクセス コントロール リストを指定するか、またはグループ ポリシーから値を継承するかどうかを指定します。フィルタは、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方法については、[Group Policy] ダイアログボックスを参照してください。ACL を表示および設定できる [ACL Manager] を開くには、[Manage] をクリックします。
- [Idle Timeout]：[Inherit] チェックボックスがオフである場合、このパラメータは、ユーザのアイドル タイムアウト時間を分単位で指定します。この期間、ユーザ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。デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。この値は、クライアントレス SSL VPN のユーザには適用されません。
- [Maximum Connect Time]：[Inherit] チェックボックスがオフである場合、このパラメータは、ユーザの最大接続時間を分単位で指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分で、最長時間は 35791394 分（4000 年超）です。接続時間を無制限にするには、[Unlimited] をオンにします（デフォルト）。

クライアント ファイアウォールを使用した VPN におけるローカル デバイスのサポートの有効化

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

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

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

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

以下の項では、次の処理を行うための手順について説明します。

- 「ローカル プリンタをサポートするためのクライアント ファイアウォールの導入」（P.3-37）
- 「VPN におけるテザー デバイスのサポートの設定」（P.3-39）

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。

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

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

ローカル印刷に関する ACL ルールの例

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

表 3-1　AnyConnect_Client_Local_Print の ACL ルール

説明	アクセス権	インターフェイス	プロトコル	送信元ポート	宛先アドレス	宛先ポート
すべて拒否	拒否	パブリック	いずれか（Any）	デフォルト	いずれか（Any）	デフォルト
LPD	許可	パブリック	TCP	デフォルト	いずれか（Any）	515
IPP	許可	パブリック	TCP	デフォルト	いずれか（Any）	631
プリンタ	許可	パブリック	TCP	デフォルト	いずれか（Any）	9100
mDNS	許可	パブリック	UDP	デフォルト	224.0.0.251	5353
LLMNR	許可	パブリック	UDP	デフォルト	224.0.0.252	5355
NetBios	許可	パブリック	TCP	デフォルト	いずれか（Any）	137
NetBios	許可	パブリック	UDP	デフォルト	いずれか（Any）	137

（注）　デフォルトのポート範囲は 1 ～ 65535 です。

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

VPN におけるローカル印刷のサポートの設定

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

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 3-1 に示した ACE を含む ACL を作成します。この ACL をプライベート ネットワーク ルールとして追加します。

ステップ 5　常時接続の自動 VPN ポリシーを有効にし、かつクローズド ポリシーを指定している場合、VPN 障害が発生するとユーザはローカル リソースにアクセスできません。このシナリオでは、**プロファイル エディタで** [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。

VPN におけるテザー デバイスのサポートの設定

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

（注）　AnyConnect を実行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。

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。

AnyConnect VPN Client 接続の設定

[Internal Group Policy] > [Advanced] > [AnyConnect Client]

[AnyConnect Client] のフィールド

- [Keep Installer on Client System]：リモート コンピュータ上で永続的なクライアントのインストールを可能にします。これをイネーブルにすることにより、クライアントの自動的なアンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモート コンピュータにインストールされたままなので、リモート ユーザの接続時間が短縮されます。
- [Compression]：圧縮を行うと、転送されるパケットのサイズが減少するため、セキュリティ アプライアンスとクライアント間の通信パフォーマンスが向上します。
- [Datagram TLS] : Datagram Transport Layer Security により、一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスを改善します。
- [Ignore Don't Defrag (DF) Bit]：この機能では、DF ビットが設定されているパケットを強制的にフラグメンテーションして、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバに対する使用などがあります。
- [Client Bypass Protocol]：クライアント プロトコル バイパス機能を使用すると、ASA が IPv6 トラフィックだけを予期しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定することができます。

  AnyConnect クライアントが ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ASA が AnyConnect 接続に IPv4 アドレスまたは IPv6 アドレスだけを割り当てた場合に、ASA が IP アドレスを割り当てなかったネットワーク トラフィックについて、クライアント プロトコル バイパスによってそのトラフィックをドロップさせるか、または ASA をバイパスしてクライアントからの暗号化なし、つまり「クリア テキスト」としての送信を許可するかを設定できるようになりました。

  たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコル機能がディセーブルの場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルがイネーブルの場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。
- [FQDN of This Device]：この情報は、VPN セッションの再確立で使用される ASA IP アドレスを解決するために、ネットワーク ローミングの後でクライアントに使用されます。この設定は、さまざまな IP プロトコルのネットワーク間のローミングをサポートするうえで重要です（IPv4 から IPv6 など）。

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

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

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

- [MTU]：SSL 接続の MTU サイズを調整します。256 ～ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLS のオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。
- [Keepalive Messages] : [Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブ メッセージの間隔をイネーブルおよび調整して、プロキシ、ファイアウォール、または NAT デバイスを通した接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモート ユーザが、Microsoft Outlook や Microsoft Internet Explorer などのソケット ベースのアプリケーションを実際に実行していないときでも、クライアントが切断と再接続を行わないことが保証されます。
- [Optional Client Modules to Download]：ダウンロード時間を最小限に抑えるために、AnyConnect クライアントは、サポートする各機能で必要とされるモジュールだけを（ASA から）ダウンロードするように要求します。次のような他の機能をイネーブルにするモジュールの名前を指定する必要があります。AnyConnect クライアントのバージョン 3.0 には、次のモジュールが含まれています（旧バージョンではモジュールの数が少なくなります）。
  - AnyConnect DART : トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システム ログのスナップショットおよびその他の診断情報がキャプチャされ、.zip ファイルがデスクトップに作成されます。
  - AnyConnect ネットワーク アクセス マネージャ：以前は Cisco Secure Services Client と呼ばれていました。このモジュールでは、802.1X（レイヤ 2）が提供され、有線ネットワークおよびワイヤレス ネットワークへのアクセスのデバイス認証が AnyConnect 3.0 に統合されます。
  - AnyConnect SBL：Start Before Logon（SBL）では、Windows のログイン ダイアログ ボックスが表示される前に AnyConnect を開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。
  - AnyConnect Web セキュリティ モジュール : 以前は ScanSafe Hostscan と呼ばれていました。このモジュールは、AnyConnect 3.0 に統合されています。
  - AnyConnect テレメトリ モジュール：悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティ アプライアンス（WSA）に送信します。WSA では、このデータを使用して、URL のフィルタリング ルールを改善します。

（注）　テレメトリ モジュールは AnyConnect バージョン 4.0 ではサポートされません。

  - AnyConnect ポスチャ モジュール：以前は Cisco Secure Desktop HostScan 機能と呼ばれていました。ポスチャ モジュールが AnyConnect 3.0 に統合され、AnyConnect で、ASA へのリモート アクセス接続を作成する前にポスチャ アセスメントのクレデンシャルを収集することができます。

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

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

  （注）　常時接続 VPN には、AnyConnect セキュア モビリティ機能をサポートする AnyConnect リリースが必要です。詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

- [Client Profiles to Download]：プロファイルは、AnyConnect クライアントで VPN、ネットワーク アクセス マネージャ、Web セキュリティ、およびテレメトリの設定に使用されるコンフィギュレーション パラメータのグループです。[Add] をクリックして [Select Anyconnect Client Profiles] ウィンドウを起動すると、グループ ポリシー用に以前に作成されたプロファイルを指定できます。

AnyConnect クライアント プロファイルの設定

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

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

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

AnyConnect クライアント プロファイルのフィールド

[Add]：[Add AnyConnect Client Profiles] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュ メモリ内のファイルをプロファイルとして指定したり、フラッシュ メモリを参照してプロファイルとして指定するファイルを表示したりできます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。

[Edit]：[Edit SSL VPN Client Profile] ウィンドウが表示されます。AnyConnect クライアント機能のプロファイルに含まれている設定を変更できます。

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

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

- [Profile Name]：プロファイルの追加時に指定されたプロファイル名。
- [Profile Usage/Type]：VPN、ネットワーク アクセス マネージャ、テレメトリなど、プロファイルの用途を表示します。

グループ ポリシーへの AnyConnect クライアント プロファイルの追加

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

フィールド

- [Profile Name] : グループ ポリシーの AnyConnect クライアント プロファイルを指定します。
- [Profile Usage]：最初に作成されたときにプロファイルに割り当てられた用途（VPN、ネットワーク アクセス マネージャ、Web セキュリティ、またはテレメトリ）を表示します。ASDM が、XML ファイルで指定された用途を認識しない場合、ドロップダウン リストが選択可能になり、用途タイプを手動で選択できます。
- [Profile Location]：ASA のフラッシュ メモリ内のプロファイル ファイルへのパスを指定します。このファイルが存在しない場合、ASA はプロファイル テンプレートに基づいてファイルを作成します。

内部グループ ポリシーへの AnyConnect クライアント プロファイルのインポート

プロファイルは、ローカル デバイスまたはリモート サーバからインポートできます。

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

フィールド

- [Profile Name]：追加するプロファイルの名前を指定します。
- [Profile Usage]：最初に作成されたときにプロファイルに割り当てられた用途（VPN、ネットワーク アクセス マネージャ、Web セキュリティ、またはテレメトリ）を表示します。ASDM が、XML ファイルで指定された用途を認識しない場合、ドロップダウン リストが選択可能になり、用途タイプを手動で選択できます。
- [Group Policy]：プロファイルのグループ ポリシーを指定します。プロファイルは、AnyConnect クライアントとともにこのグループ ポリシーに属しているユーザにダウンロードされます。
- [Profile Location]：ASA のフラッシュ メモリ内のプロファイル ファイルへのパスを指定します。このファイルが存在しない場合、ASA はプロファイル テンプレートに基づいてファイルを作成します。

AnyConnect クライアント プロファイルのエクスポート

このウィンドウから AnyConnect VPN クライアント プロファイルをエクスポートします。プロファイルは、ローカル デバイスまたはリモート サーバにエクスポートできます。

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

フィールド

[Device Profile Path]：プロファイル ファイルのパスおよびファイル名を表示します。

[Local Path]：パスとファイル名を指定してプロファイル ファイルをエクスポートします。

[Browse Local]：クリックしてウィンドウを起動し、ローカル デバイス ファイル システムを参照します。

AnyConnect トラフィックに対するネットワーク アドレス変換の免除

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

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

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

表 3-2　VPN クライアントのアイデンティティ NAT を設定するネットワーク アドレス アドレッシング

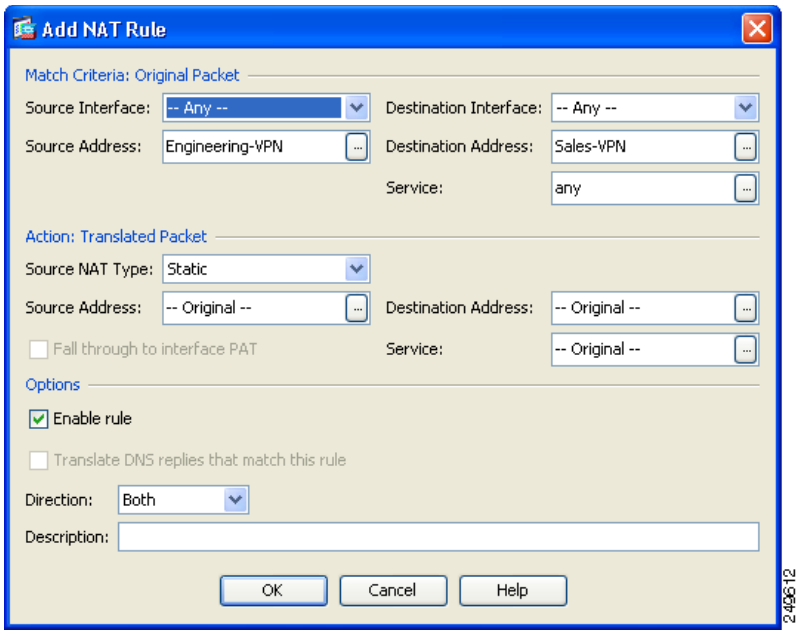
ネットワークまたはアドレス プール	ネットワーク名またはアドレス プール名	アドレス範囲
内部ネットワーク	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN アドレス プール	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN アドレス プール	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ ネットワーク	DMZ-network	192.168.1.0 - 192.168.1.255

ステップ 1　ASDM にログインし、[Configuration] > [Firewall] > [NAT Rules] に移動します。

ステップ 2　Engineering VPN アドレス プールのホストが Sales VPN アドレス プールのホストに接続できるよう、NAT 規則を作成します。ASA が Unified NAT テーブルの他の規則の前にこの規則を評価するよう、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] に移動します。

（注）　NAT ルールはトップダウン方式で最初に一致したルールから順に適用されます。いったんパケットが特定の NAT 規則と一致すると、それ以上評価は行われません。ASA が NAT 規則を早まって広範な NAT 規則に一致しないよう、Unified NAT テーブルの先頭に最も固有の NAT 規則を配置することが重要です。

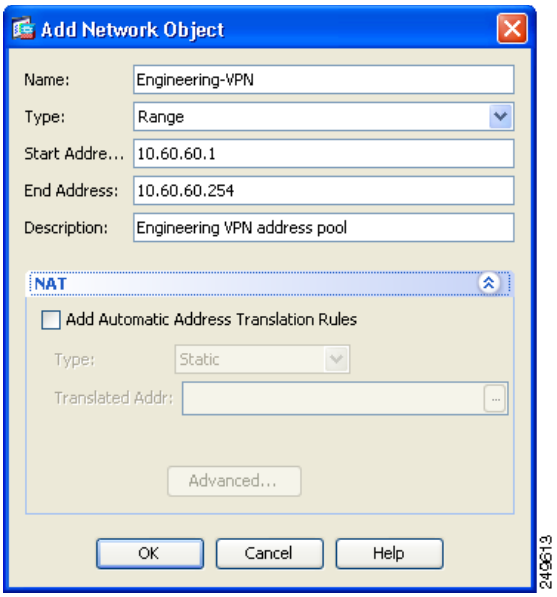
図 3-2　[Add NAT rule] ダイアログ ボックス



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

- [Source Interface]：Any
- [Destination Interface]：Any
- [Source Address]：[Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの**範囲**として定義します。自動アドレス トランスレーション ルールは追加しないでください。例については、図 3-3 を参照してください。
- [Destination Address]：[Destination Address] ブラウズ ボタンをクリックし、Sales VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの**範囲**として定義します。自動アドレス トランスレーション ルールは追加しないでください。

図 3-3　VPN アドレス プールのネットワーク オブジェクトの作成



b. [Action Translated Packet] エリアで、次のフィールドを設定します。
   - [Source NAT Type]：Static
   - [Source Address]：Original
   - [Destination Address]：Original
   - [Service]：Original

c. [Options] エリアで、次のフィールドを設定します。
   - [Enable rule] をオンにします。
   - [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
   - [Direction]：Both
   - [Description]：規則の説明を入力します。

d. [OK] をクリックします。

e. [Apply] をクリックします。規則は図 3-5（P.3-49）の 「Unified NAT テーブル」の規則 1 のようになるはずです。

   CLI の例：

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

f. [Send] をクリックします。

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

CLI の例：

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

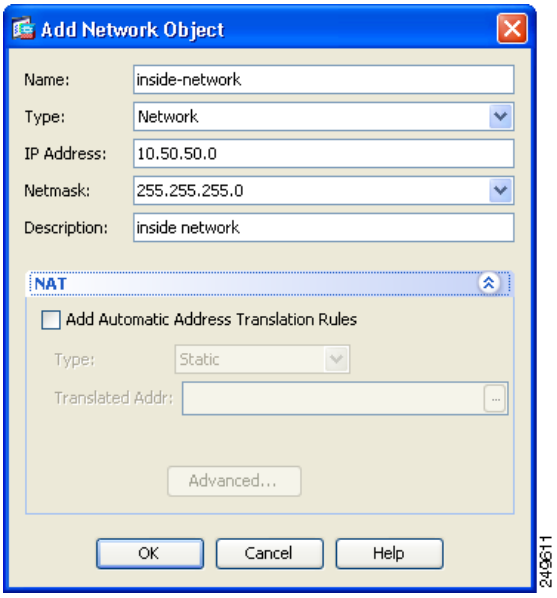
ステップ 4　Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。ステップ 2 で規則を作成したときのようにこの規則を作成します。ただし、[Match criteria: Original Packet] エリアで Engineering VPN アドレス プールを送信元アドレスおよび宛先アドレス両方として指定します。

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

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

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

図 3-4　inside-network オブジェクトの追加



b. [Action Translated Packet] エリアで、次のフィールドを設定します。

- [Source NAT Type]：Static
- [Source Address]：Original
- [Destination Address]：Original
- [Service]：Original

c. [Options] エリアで、次のフィールドを設定します。

- [Enable rule] をオンにします。
- [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
- [Direction]：Both
- [Description]：規則の説明を入力します。

d. [OK] をクリックします。

e. [Apply] をクリックします。規則は図 3-5（P.3-49）の 「Unified NAT テーブル」の規則 2 のようになるはずです。

CLI の例

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

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

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

a. この規則が他の規則の前に処理されるよう [NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。

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

- [Source Interface]：Any
- [Destination Interface]：Any。[Action: Translated Packet] エリアの [Source Address] に [outside] を選択すると、このフィールドには自動的に「outside」が入力されます。
- [Source Address]：[Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。
- [Destination Address]：Any

c. [Action Translated Packet] エリアで、次のフィールドを設定します。

- [Source NAT Type]：Dynamic PAT (Hide)
- [Source Address]：[Source Address] ブラウズ ボタンをクリックし、outside インターフェイスを選択します。
- [Destination Address]：Original
- [Service]：Original

d. [Options] エリアで、次のフィールドを設定します。

- [Enable rule] をオンにします。
- [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
- [Direction]：Both
- [Description]：規則の説明を入力します。

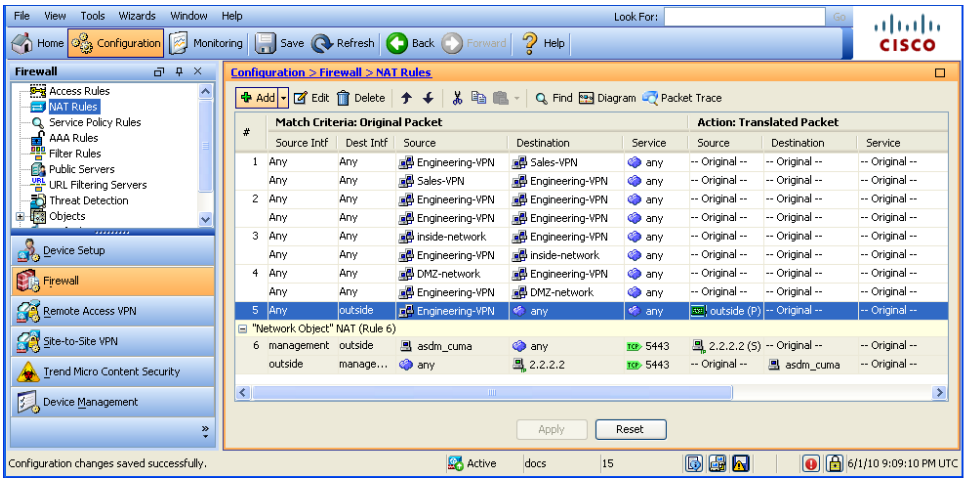
e. [OK] をクリックします。

f. [Apply] をクリックします。規則は図 3-5（P.3-49）の 「Unified NAT テーブル」の規則 5 のようになるはずです。

CLI の例：

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

図 3-5　Unified NAT テーブル



ステップ 8　Engineering VPN アドレス プールがそのプール自体、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネットに到達するように設定した後に、Sales VPN アドレス プールについて同じプロセスを繰り返す必要があります。アイデンティティ NAT を使用して、Sales VPN アドレス プール トラフィックが、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネット間のネットワーク アドレス変換の対象外となるようにします。

ステップ 9　ASA の [File] メニューで [Save Running Configuration to Flash] を選択し、アイデンティティ NAT 規則を実装します。

接続プロファイルについて

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

AnyConnect 接続プロファイル：メイン ペイン

メイン ペインでは、選択するインターフェイスでのクライアント アクセスをイネーブルにし、接続プロファイル（トンネル グループ）を選択、追加、編集、および削除できます。ログイン時にユーザが特定の接続を選択できるようにするかどうかも指定できます。

フィールド

- [Access Interfaces]：アクセスをイネーブルにするインターフェイスをテーブルから選択できます。このテーブルのフィールドには、インターフェイス名やチェックボックスが表示され、アクセスを許可するかどうかを指定します。
  - インターフェイス テーブルの AnyConnect 接続に設定するインターフェイスの行で、インターフェイスでイネーブルにするプロトコルをオンにします。SSL アクセス、IPSec アクセス、またはその両方を許可できます。

SSL をオンにすると、DTLS（Datagram Transport Layer Security）がデフォルトでイネーブルになります。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

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

- [Device Certificate]：RSA キーまたは ECDSA キーの認証の証明書を指定できます。「デバイス証明書の指定」（P.3-51）を参照してください。
- [Port Setting]：HTTPS および DTLS（RA クライアントのみ）接続のポート番号を設定します。「接続プロファイルでのポート設定」（P.3-51）を参照してください。
- [Bypass interface access lists for inbound VPN sessions]：[Enable inbound VPN sessions to bypass interface ACLs] がデフォルトでオンになっています。セキュリティ アプライアンスが、すべての VPN トラフィックのインターフェイス ACL の通過を許可します。たとえば、外部インターフェイス ACL が復号化されたトラフィックの通過を許可しない場合でも、セキュリティ アプライアンスはリモート プライベート ネットワークを信頼し、復号化されたパケットの通過を許可します。このデフォルトの動作を変更できます。インターフェイス ACL に VPN 保護対象トラフィックの検査を行わせるためには、このチェックボックスをオフにします。

- [Login Page Setting]
  - ユーザはそのエイリアスで識別される接続プロファイルをログイン ページで選択できます。このチェックボックスをオンにしない場合、デフォルト接続プロファイルは DefaultWebVPNGroup です。
  - [Shutdown portal login page.]：ログインがディセーブルの場合に Web ページを表示します。
- [Connection Profiles]：接続（トンネル グループ）のプロトコル固有属性を設定します。
  - [Add/Edit]：接続プロファイル（トンネル グループ）を追加または編集します。
  - [Name]：接続プロファイルの名前。
  - [Aliases]：接続プロファイルの別名。
  - [SSL VPN Client Protocol]：SSL VPN クライアントにアクセス権を与えるかどうかを指定します。
  - [Group Policy]：この接続プロファイルのデフォルト グループ ポリシーを表示します。
  - [Allow user to choose connection, identified by alias in the table above, at login page]：[Login] ページでの接続プロファイル（トンネル グループ）エイリアスの表示をイネーブルにする場合はオンにします。
- [Let group URL take precedence if group URL and certificate map match different connection profiles.Otherwise, the connection profile matches the certificate map will be used.]：このオプションでは、接続プロファイルの選択プロセス時にグループ URL および証明書の値の相対的プリファレンスを指定します。ASA で、推奨される値と一致する値が見つからない場合は、別の値に一致する接続プロファイルが選択されます。VPN エンドポイントで指定したグループ URL を、同じグループ URL を指定する接続プロファイルと照合するために、多数の古い ASA ソフトウェア リリースで使用されるプリファレンスを利用する場合にのみ、このオプションをオンにします。このオプションは、デフォルトではオフになっています。オフにした場合、ASA は接続プロファイルで指定した証明書フィールド値を、エンドポイントで使用する証明書のフィールド値と照合して、接続プロファイルを割り当てます。

デバイス証明書の指定

[Specify Device Certificate] 画面を使用すると、接続を作成しようとした場合に、クライアントに ASA を特定する証明書を指定できます。この画面は、AnyConnect 接続プロファイルおよびクライアントレス接続プロファイル用です。

リモート アクセス VPN の制限事項

- Always-on IPsec/IKEv2 などの特定の AnyConnect 機能では、有効で信頼できるデバイスの証明書を ASA で利用できる必要があります。
- AnyConnect クライアントが SSL のみを使用するように設定されている場合は、AnyConnect は SSL VPN の ECDSA の証明書をサポートしていないので、RSA の証明書の指定だけが必要になります。AnyConnect クライアントが IPSec または SSL を使用するように設定されている場合は、どちらの種類の証明書も設定できます。
- ECDSA の証明書は、IPSec 接続だけでサポートされます。

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

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

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

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

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

ステップ 4　[OK] をクリックします。

接続プロファイルでのポート設定

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

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

[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles]

フィールド

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

AnyConnect 接続プロファイル：基本属性

AnyConnect VPN 接続の基本属性を設定するには、[Connection Profiles] セクションで [Add] または [Edit] を選択します。[Add/Edit AnyConnect Connection Profile] > [Basic] ダイアログボックスが開きます。

フィールド

[Add AnyConnect Connection Profile] > [Basic] ダイアログボックスで次の属性を設定します。

- [Name]：[Add] の場合、追加する接続プロファイルの名前を指定します。[Edit] の場合、このフィールドは編集できません。
- [Aliases]：（オプション）この接続の代替名を 1 つ以上入力します。名前は、スペースまたは句読点で区切ることができます。
- [Authentication]：認識の方法を、次の中から 1 つ選択し、認証処理で使用する AAA サーバ グループを指定します。
  - AAA、Certificate、または Both：AAA、Certificate、または Both から使用する認証処理の種類を選択します。Certificate または Both を選択すると、ユーザは接続するために証明書を入力する必要があります。
  - [AAA Server Group]：ドロップダウン リストから AAA サーバ グループを選択します。デフォルト設定は LOCAL です。この場合は、ASA が認証を処理するように指定されます。選択する前に、[Manage] をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、AAA サーバ グループの ASA コンフィギュレーションを表示したり、変更を加えたりすることができます。
  - LOCAL 以外のグループを選択すると、[Use LOCAL if Server Group Fails] チェックボックスが選択できるようになります。
  - [Use LOCAL if Server Group fails]：[Authentication Server Group] 属性によって指定されたグループに障害が発生したときに、LOCAL データベースをイネーブルにする場合はオンにします。
- [Client Address Assignment]：使用する DHCP サーバ、クライアント アドレス プール、クライアント IPv6 アドレス プールを選択します。
  - [DHCP Servers]：使用する DHCP サーバの名前または IP アドレスを入力します。
  - [Client Address Pools]：クライアント アドレス割り当てで使用する、選択可能な設定済みの IPv4 アドレス プールの名前を入力します。選択する前に、[Select] をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、アドレス プールを表示したり、変更を加えたりすることができます。IPv4 アドレス プールを追加または編集する方法の詳細については「ローカル IP アドレス プールの設定」（P.4-3）を参照してください。
  - [Client IPv6 Address Pools]：クライアント アドレス割り当てで使用する、選択可能な設定済みの IPv6 アドレス プールの名前を入力します。選択する前に、[Select] をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、アドレス プールを表示したり、変更を加えたりすることができます。IPv6 アドレス プールを追加または編集する方法の詳細については「ローカル IP アドレス プールの設定」（P.4-3）を参照してください。
- [Default Group Policy]：使用するグループ ポリシーを選択します。
  - [Group Policy]：この接続のデフォルト グループ ポリシーとして割り当てる VPN グループ ポリシーを選択します。VPN グループ ポリシーは、ユーザ指向属性値のペアの集合で、デバイスで内部に、または RADIUS サーバで外部に保存できます。デフォルト値は DfltGrpPolicy です。[Manage] をクリックして別のダイアログボックスを重ねて開き、グループ ポリシー コンフィギュレーションに変更を加えることができます。

- [Enable SSL VPN client protocol]：VPN 接続の SSL をイネーブルにする場合にオンにします。
- [Enable IPsec (IKEv2) client protocol]：接続で IKEv2 を使用する IPsec をイネーブルにする場合にオンにします。
- [DNS Servers]：ポリシーの DNS サーバの IP アドレスを入力します（1 つまたは複数）。
- [WINS Servers]：ポリシーの WINS サーバの IP アドレスを入力します（1 つまたは複数）。
- [Domain]：デフォルトのドメイン名を入力します。

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

AnyConnect 接続プロファイル：詳細属性

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

- 一般属性
- クライアント アドレス指定属性
- 認証属性
- 認可属性
- アカウンティング属性
- ネーム サーバ属性
- クライアントレス SSL VPN 属性

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

AnyConnect 接続プロファイル：一般属性

フィールド

- [Enable Simple Certificate Enrollment (SCEP) for this Connection Profile]
- [Strip the realm from username before passing it on to the AAA server]
- [Strip the group from username before passing it on to the AAA server]
- [Group Delimiter]

パスワード管理

- [Enable Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

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

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

どちらの場合でも、変更されずにパスワードが期限切れになると、ASA はパスワードを変更する機会をユーザに提供します。現在のパスワードの期限が切れていなければ、ユーザはそのパスワードで引き続きログインできます。

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

– [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

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

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

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

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

接続プロファイルでのクライアント アドレス指定の設定

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

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles]
- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles]
- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles]

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

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

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

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

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

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

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

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

次の各項では、アドレス プールを設定する [Add] ダイアログのフィールドについて説明します。

- 「接続プロファイルでのインターフェイスへのアドレス プールの割り当て」
- 「[Select Address Pools]」
- 「[Add or Edit IP Pool]」

接続プロファイルでのインターフェイスへのアドレス プールの割り当て

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

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

[Select Address Pools]

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

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

[Add or Edit IP Pool]

[Add or Edit IP Pool] ダイアログボックスでは、クライアント アドレス割り当てで使用する IP アドレスの範囲を指定または変更できます。

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

AnyConnect 接続プロファイル：認証属性

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

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

  プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（役職）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。

- [Primary Field]：ユーザ名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field] は無視されます。
- [Secondary Field]：[Primary Field] が指定されていない場合、使用するフィールドを選択します。

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

AnyConnect 接続プロファイル：2 次認証属性

[Secondary Authentication] ダイアログボックスを使用して、この接続プロファイルに対して 2 次認証または「二重」認証を設定できます。二重認証をイネーブルにすると、エンド ユーザはログオンするために有効な認証クレデンシャルが 2 セット必要です。証明書のユーザ名の事前入力と 2 次認証を組み合わせて使用できます。このダイアログボックスのフィールドは、1 次認証で設定するフィールドと似ていますが、これらのフィールドは 2 次認証にだけ関連します。

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

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

フィールド

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

    （注） この接続プロファイルの認証サーバも指定した場合でも、認証サーバ設定が優先されます。ASA は、このセカンダリ認証サーバを無視します。

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

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

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

属性	定義
C	Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。

属性	定義
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（役職）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。

- [Use the entire DN as the username]：完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得します。
- [Use script to select username]：デジタル証明書からユーザ名を抽出するスクリプトを指定します。デフォルトは [None] です。
  - [Add or Edit]：[Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザ名のマッピングに使用するスクリプトを定義できます。
  - [Delete]：選択したスクリプトを削除します。確認されず、やり直しもできません。

AnyConnect 接続プロファイル：認可属性

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

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

[Authorization Server Group] のフィールド

- [Authorization Server Group]：認可パラメータを記述する認可サーバ グループを指定します。
  - [Server Group]：使用する認可サーバ グループを選択します。デフォルトは none です。
  - [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。AAA サーバの設定については、「クライアントレス SSL VPN 接続プロファイルでのインターフェイスへの認証サーバ グループの割り当て」（P.3-69）を参照してください。
  - [Users must exist in the authorization database to connect]：ユーザがこの基準を満たす必要がある場合は、このチェックボックスをオンにします。
- [Interface-specific Authorization Server Groups]：指定のインターフェイスに対する認可サーバ グループの割り当てを管理します。
  - [Add or Edit]：[Assign Authentication Server Group to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバ グループを指定するとともに、選択したサーバ グループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。
  - [Delete]：選択したサーバ グループをテーブルから削除します。確認されず、やり直しもできません。

- [Username Mapping from Certificate]：ユーザ名を抽出するデジタル証明書のフィールドを指定できます。
  - [Use script to select username]：デジタル証明書からユーザ名を選択する場合に使用するスクリプト名を指定します。デフォルトは [None] です。証明書フィールドからユーザ名を選択するスクリプトを作成する方法の詳細については、「証明書のユーザ名事前入力のためにユーザ名を選択するスクリプト コンテンツの追加」（P.3-61）を参照してください。
  - [Add or Edit]：[Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザ名のマッピングに使用するスクリプトを定義できます。
  - [Delete]：選択したスクリプトを削除します。確認されず、やり直しもできません。
  - [Use the entire DN as the username]：証明書の [Distinguished Name] フィールド全体をユーザ名として使用する場合に指定します。
  - [Specify the certificate fields to be used as the username]：ユーザ名に結合する 1 つ以上のフィールドを指定します。
  - [Primary Field]：ユーザ名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field] は無視されます。
  - [Secondary Field]：[Primary Field] が指定されていない場合、使用するフィールドを選択します。
- [Find]：検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

証明書のユーザ名事前入力のためにユーザ名を選択するスクリプト コンテンツの追加

スクリプトを使用してユーザ名を選択する場合は、他のマッピング オプションのリストに表示されていない認可用の証明書フィールドを使用するスクリプトを作成または編集します。

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

フィールド

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

  たとえば、ホスト/ユーザの値を含む DN 属性の Common Name（CN）を選択したとします。表 3-3 には、さまざまな戻り値を実現する部分文字列を使用してこの値をフィルタする方法がいくつか示されています。戻り値は、ユーザ名として実際に事前入力される値です。

表 3-3　部分文字列によるフィルタリング

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

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

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

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

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

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

表 3-4 に Lua スクリプトで使用できる属性名と説明を示します。

（注） Lua では大文字と小文字が区別されます。

表 3-4　属性名と説明

属性名	説明
cert.subject.c	国
cert.subject.cn	一般名
cert.subject.dnq	DN 修飾子
cert.subject.ea	電子メール アドレス
cert.subject.genq	世代修飾子
cert.subject.gn	名
cert.subject.i	イニシャル
cert.subject.l	地名
cert.subject.n	名前
cert.subject.o	組織
cert.subject.ou	組織単位

表 3-4　　属性名と説明

cert.subject.ser	サブジェクト シリアル番号
cert.subject.sn	姓
cert.subject.sp	州/県
cert.subject.t	役職
cert.subject.uid	ユーザ ID
cert.issuer.c	国
cert.issuer.cn	一般名
cert.issuer.dnq	DN 修飾子
cert.issuer.ea	電子メール アドレス
cert.issuer.genq	世代修飾子
cert.issuer.gn	名
cert.issuer.i	イニシャル
cert.issuer.l	地名
cert.issuer.n	名前
cert.issuer.o	組織
cert.issuer.ou	組織単位
cert.issuer.ser	発行元シリアル番号
cert.issuer.sn	姓
cert.issuer.sp	州/県
cert.issuer.t	役職
cert.issuer.uid	ユーザ ID
cert.serialnumber	証明書シリアル番号
cert.subjectaltname.upn	ユーザ プリンシパル名

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

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

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

フィールド

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

接続プロファイルでのアカウンティングの設定

このダイアログボックスでの設定は、ASA 全体の接続プロファイル（トンネル グループ）にグローバルに適用されます。このダイアログボックスでは、次の属性を設定できます。

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

AnyConnect 接続プロファイルでのエイリアスと URL の設定

このダイアログボックスでは、ログイン時のリモート ユーザの画面に影響する属性を設定します。このダイアログのフィールドは AnyConnect クライアントおよびクライアントレス SSL VPN で同じですが、クライアントレス SSL VPN には追加のフィールドが 1 つあります。接続プロファイルのタブの名前は、AnyConnect では [Group URL/Group Alias] で、クライアントレス SSL VPN では [Clientless SSL VPN] です。

接続エイリアスとグループ URL のフィールド

- [Enable the display of Radius Reject-Message on the login screen]：認証が拒否された場合に「Radius-Reject」メッセージをログイン画面に表示するには、このチェックボックスをオンにします。
- [Enable the display of SecurId message on the login screen]：ログイン ダイアログボックスに「SecurID」メッセージを表示するにはこのチェックボックスをオンにします。
- [Manage]：[Configure GUI Customization Objects] ダイアログボックスが開きます。
- [Connection Aliases]：既存の接続エイリアスとそのステータスの一覧がテーブルに表示されます。各項目をテーブルに追加したり、テーブルから削除したりできます。ログイン時にユーザが特定の接続（トンネル グループ）を選択できるように接続が設定されている場合は、ユーザのログイン ページに接続エイリアスが表示されます。このテーブルの行は編集できるため、[Edit] ボタンはありません。テーブルの上の「i」アイコンをクリックすると、編集機能のツールヒントが表示されます。
  - [Add]：[Add Connection Alias] ダイアログボックスが開きます。このダイアログボックスでは、接続エイリアスを追加し、イネーブルにすることができます。
  - [Delete]：選択した行を接続エイリアス テーブルから削除します。確認されず、やり直しもできません。
  - テーブルに表示されているエイリアスを編集するには、行をダブルクリックします。
- [Group URLs]：既存のグループ URL とそのステータスの一覧がテーブルに表示されます。各項目をテーブルに追加したり、テーブルから削除したりできます。ログイン時にユーザが特定のグループを選択できるように接続が設定されている場合は、ユーザのログイン ページにグループ URL が表示されます。このテーブルの行は編集できるため、[Edit] ボタンはありません。テーブルの上の「i」アイコンをクリックすると、編集機能のツールヒントが表示されます。
  - [Add]：[Add Group URL] ダイアログボックスが開きます。このダイアログボックスでは、グループ URL を追加し、イネーブルにすることができます。
  - [Delete]：選択した行を接続エイリアス テーブルから削除します。確認されず、やり直しもできません。
  - テーブルに表示されている URL を編集するには、行をダブルクリックします。

- [Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA.(If a client connects using a connection alias, this setting is ignored.)] : [Group URLs] テーブルのエントリに一致する URL を使用する CSD を実行しないようにする場合、オンにします。このオプションをオンにすると、セキュリティ アプライアンスがこれらのユーザからエンドポイント基準を受信しないようにするため、ユーザに VPN アクセスを提供するよう DAP 設定を変更する必要があります。

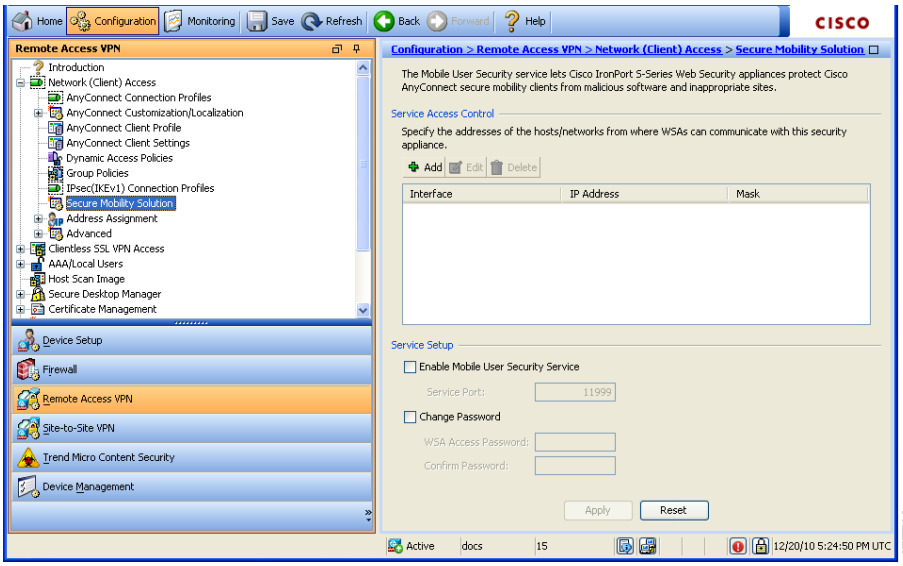
AnyConnect セキュア モビリティの設定

AnyConnect セキュア モビリティは、従業員の移動時に企業の利益と資産をインターネットの脅威から保護します。[Mobile User Security] ダイアログボックスを使用して、この機能を設定します。AnyConnect Secure Mobility により Cisco IronPort S シリーズ Web セキュリティ アプライアンスは Cisco AnyConnect セキュア モビリティ クライアントをスキャンでき、クライアントを悪意あるソフトウェアや不適切なサイトから確実に保護します。クライアントは、Cisco IronPort S シリーズ Web セキュリティ アプライアンス保護がイネーブルになっているか定期的に確認します。

セキュア モビリティ ソリューションを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Mobile User Security] を選択します。

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

図 3-6　[Mobile User Security] ウィンドウ



フィールド

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

Add or Edit MUS Access Control

[Add or Edit MUS Access Control] ダイアログボックスにより MUS アクセスを設定できます。

フィールド

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

クライアントレス SSL VPN 接続プロファイルの設定

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

[Connection Profiles] ペインのフィールド

- [Access Interfaces]：アクセスでイネーブルにするインターフェイスを選択できます。このテーブルのフィールドには、インターフェイス名やチェックボックスが表示され、アクセスを許可するかどうかを指定します。
  - [Device Certificate]：RSA キーまたは ECDSA キーまたはトラストポイントの認証の証明書を指定できます。2 つのトラストポイントを設定するオプションがあります。クライアントは、ベンダー ID ペイロードによる ECDSA のサポートを示します。ASA は、設定したトラストポイント リストをスキャンし、クライアントがサポートする最初の 1 つを選択します。ECDSA を使用する場合は、RSA トラストポイントの前に、このトラストポイントを設定する必要があります。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、選択した証明書の詳細を追加、編集、削除、エクスポート、または表示できます。
  - [Port Setting]：クライアントレス SSL および IPsec（IKEv2）接続のポート番号を設定します。範囲は 1 ～ 65535 です。デフォルトはポート 443 です。
- [Login Page Setting]
  - エイリアスで識別される接続プロファイルをログイン ページで選択できます。選択しない場合は、DefaultWebVPNGroup が接続プロファイルになります。ユーザのログイン ページに、ユーザが接続で使用する特定のトンネル グループを選択するためのドロップダウン リストが表示されるように指定します。
  - [Allow user to enter internal password on the login page]：内部サーバへのアクセス時に異なるパスワードを入力するオプションを追加します。
  - [Shutdown portal login page]：ログインがディセーブルの場合に Web ページを表示します。
- [Connection Profiles]：この接続（トンネル グループ）の接続ポリシーを決定するレコードを示した接続テーブルを表示します。各レコードによって、その接続のデフォルト グループ ポリシーが識別されます。レコードには、プロトコル固有の接続パラメータが含まれています。
  - [Add]：選択した接続の [Add Clientless SSL VPN] ダイアログボックスが開きます。
  - [Edit]：選択した接続の [Edit Clientless SSL VPN] ダイアログボックスが開きます。
  - [Delete]：選択した接続をテーブルから削除します。確認されず、やり直しもできません。
  - [Name]：接続プロファイルの名前。
  - [Enabled]：イネーブルになっている場合にチェックマークが付きます。
  - [Aliases]：接続プロファイルの別名。
  - [Authentication Method]：使用する認証方式を指定します。
  - [Group Policy]：この接続プロファイルのデフォルト グループ ポリシーを表示します。
- [Let group URL take precedence if group URL and certificate map match different connection profiles.Otherwise, the connection profile matches the certificate map will be used.]：このオプションでは、接続プロファイルの選択プロセス時にグループ URL および証明書の値の相対的プリファレンスを指定します。ASA で、エンドポイントによって指定された推奨される値を、接続プロファイルによって指定された推奨される値と照合できない場合は、別の値と一致する接続プロファイルが選択されます。VPN エンドポイントで指定したグループ URL を、同じグループ URL を指定する接続プロファイルと照合するために、多数の古い ASA ソフトウェア リリースで使用されるプリファレンスを利用する場合にのみ、このオプションをオンにします。このオプションは、デフォルトではオフになっています。オフにした場合、ASA は接続プロファイルで指定した証明書フィールド値を、エンドポイントで使用する証明書のフィールド値と照合して、接続プロファイルを割り当てます。

クライアントレス SSL VPN 接続プロファイルでの基本属性の設定

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

[Basic] ペインのフィールド

- [Name]：接続名を指定します。編集機能の場合、このフィールドは読み取り専用です。
- [Aliases]：（オプション）この接続の代替名を 1 つ以上指定します。[Clientless SSL VPN Access Connections] ダイアログボックスでそのオプションを設定している場合に、ログイン ページに別名が表示されます。
- [Authentication]：認証パラメータを指定します。
  - [Method]：この接続で、AAA 認証、証明書認証、またはその両方を使用するかどうかを指定します。デフォルトは AAA 認証です。
  - [AAA server Group]：この接続の認証処理で使用する AAA サーバ グループを選択します。デフォルトは LOCAL です。
  - [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。
- [DNS Server Group] : この接続の DNS サーバ グループとして使用するサーバを選択します。デフォルトは DefaultDNS です。
- [Default Group Policy]：この接続で使用するデフォルト グループ ポリシーのパラメータを指定します。
  - [Group Policy]：この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。
  - [Clientless SSL VPN Protocol]：この接続でのクライアントレス SSL VPN プロトコルをイネーブルまたはディセーブルにします。

クライアントレス SSL VPN 接続プロファイルでの一般属性の設定

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

[General Attributes] ペインのフィールド

- [Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - [Enable notification password management]：このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザに通知するか、またはパスワードが期限切れになる当日にユーザに通知するかを決定します。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ～ 180 日です。

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

どちらの場合でも、変更されずにパスワードが期限切れになると、ASA はパスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

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

– [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

クライアントレス SSL VPN 接続プロファイルでの認証の設定

[Clientless SSL VPN Connection Profile] > [Advanced] > [Authentication] ダイアログボックスでは、インターフェイス固有の認可サーバ グループを表示、追加、編集、または削除できます。このダイアログボックスのテーブルの各行には、インターフェイス固有サーバ グループのステータスが表示されます。表示されるのは、インターフェイス名、それに関連付けられたサーバ グループ、および選択したサーバ グループで障害が発生したときにローカル データベースへのフォールバックがイネーブルになっているかどうかです。

[Authentication] ペインのフィールドは、「AnyConnect 接続プロファイル：認証属性」（P.3-56）で説明した AnyConnect 認証の場合と同じです。

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

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

この設定を行うフィールドについては、「クライアントレス SSL VPN 接続プロファイルでのインターフェイスへの認可サーバ グループの割り当て」（P.3-63）を参照してください。

クライアントレス SSL VPN 接続プロファイルでの 2 次認証の設定

クライアントレス SSL の 2 次認証設定フィールドは、「AnyConnect 接続プロファイル：2 次認証属性」（P.3-58）で説明した AnyConnect クライアント アクセスの場合と同じです。

クライアントレス SSL VPN 接続プロファイルでの認可の設定

クライアントレス SSL の認可設定フィールドは、AnyConnect、IKEv1、および IKEv2 の場合と同じです。これらのフィールドの詳細については、「AnyConnect 接続プロファイル：認可属性」（P.3-60）を参照してください。

クライアントレス SSL VPN 接続プロファイルでの NetBIOS サーバの設定

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

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

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

[NetBIOS Servers] ペインのフィールド

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

クライアントレス SSL VPN 接続プロファイルでのグループ URL とエイリアスの設定

クライアントレス接続プロファイルの [Advanced] > [Clientless SSL VPN] ペインでは、ログイン時のリモート ユーザの画面に影響する属性を設定できます。

フィールド

- [Portal Page Customization(Clientless SSL VPN only)]：適用する事前設定されたカスタマイゼーション属性を指定することにより、ユーザのログイン ページのルックアンドフィールを設定します。デフォルトは DfltCustomization です。

このダイアログの残りのフィールドは、AnyConnect 接続プロファイルの場合と同じです。詳細については、「AnyConnect 接続プロファイルでのエイリアスと URL の設定」（P.3-64）を参照してください。

DNS サーバ グループの設定

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

フィールド

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

IKEv1 接続プロファイル

このペインでは、L2TP-IPsec を含む IKEv1 クライアントの接続プロファイルを設定します。

[Connection Profile] ペインのフィールド

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

- [L2TP/IPsec Enabled]：L2TP/IPsec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPsec Remote Access Connection] の [Basic] ダイアログボックスでイネーブルにします。
- [Authentication Server Group]：認証を提供できるサーバ グループの名前。
- [Group Policy]：この IPsec 接続のグループ ポリシーの名前を示します。

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

IPsec リモート アクセス接続プロファイルの設定：[Basic] タブ

[Add or Edit IPsec Remote Access Connection Profile Basic] ダイアログボックスでは、L2TP-IPsec を含む IPsec IKEv1 VPN 接続の共通属性を設定できます。

IPsec 接続プロファイルの [Basic] タブのフィールド

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

クライアント アドレス指定の設定

クライアント アドレス指定の設定はすべてのクライアント接続プロファイルに共通です。詳細については、「接続プロファイルでのクライアント アドレス指定の設定」（P.3-54）を参照してください。

認証の設定

認証の設定はすべてのクライアント接続プロファイルに共通です。詳細については、「AnyConnect 接続プロファイル：認証属性」（P.3-56）を参照してください。

認可の設定

認可の設定はすべてのクライアント接続プロファイルに共通です。詳細については、「AnyConnect 接続プロファイル：認証属性」（P.3-56）を参照してください。

アカウンティングの設定

アカウンティングの設定はすべてのクライアント接続プロファイルに共通です。詳細を参照してください。

IKEv1 接続プロファイルでの IPsec の設定

ヘルプ リンクが Site-to-Site リストにあるため、さらに作業が必要です。

IKEv1 接続プロファイルでの PPP の設定

この IKEv1 接続プロファイルを使用して PPP 接続で許可される認証プロトコルを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] を開いて、いずれかの接続プロファイルを追加または編集します。

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

[PPP] ペインのフィールド

- [CHAP]：PPP 接続で CHAP プロトコルの使用をイネーブルにします。
- [MS-CHAP-V1]：PPP 接続で MS-CHAP-V1 プロトコルの使用をイネーブルにします。
- [MS-CHAP-V2]：PPP 接続で MS-CHAP-V2 プロトコルの使用をイネーブルにします。
- [PAP]：PPP 接続で PAP プロトコルの使用をイネーブルにします。
- [EAP-PROXY]：PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。EAP は、Extensible Authentication protocol（拡張認証プロトコル）を意味します。

サードパーティおよびネイティブの VPN の IKEv2 接続プロファイル

IKEv2 接続プロファイルでは、ネイティブおよびサードパーティの VPN クライアントに対して EAP、証明書ベース、および事前共有キー ベースの認証を定義します。ASDM の設定パネルは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles] です。

フィールド

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

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

IPsec IKEv2 接続プロファイルの追加または編集：[Basic] タブ

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

フィールド

- [Name]：接続名を指定します。
- [IKE Peer Authentication]：IKE ピアを設定します。
  - [Pre-shared key]：接続の事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Enable Certificate Authentication]：オンにすると、認証に証明書を使用できます。
  - [Enable peer authentication using EAP]：オンにすると、認証に EAP を使用できます。このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。
  - [Send an EAP identity request to the client] : リモート アクセス VPN クライアントに EAP 認証要求を送信できます。

  - [Identity Certificate]：ID 証明書が設定および登録されている場合は、ID 証明書の名前を選択します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、選択した証明書の詳細を追加、編集、削除、エクスポート、または表示できます。
- [User Authentication]：ユーザ認証で使用するサーバの情報を指定します。詳細な認証情報は [Advanced] セクションで設定できます。
  - [Server Group]：ユーザ認証で使用するサーバ グループを選択します。デフォルトは LOCAL です。LOCAL 以外のサーバ グループを選択すると、[Fallback] チェックボックスが選択できるようになります。
  - [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。
  - [Fallback]：指定したサーバ グループで障害が発生した場合に、ユーザ認証で LOCAL を使用するかどうかを指定します。
- [Client Address Assignment]：クライアント属性の割り当てに関連した属性を指定します。
  - [DHCP Servers]：使用する DHCP サーバの IP アドレスを指定します。最大で 10 台までのサーバをスペースで区切って追加できます。
  - [Client Address Pools]：事前定義済みのアドレス プールを 6 個まで指定します。アドレス プールを定義するには、[Configuration] > [Remote Access VPN] > [Network Client Access] > [Address Assignment] > [Address Pools] に移動します。
  - [Select]：[Select Address Pools] ダイアログボックスが開きます。
- [Default Group Policy]：デフォルト グループ ポリシーに関連した属性を指定します。
  - [Group Policy]：この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。
  - [Manage]：[Configure Group Policies] ダイアログボックスが開きます。このダイアログボックスでは、グループ ポリシーを追加、編集、または削除できます。
  - [Client Protocols]：この接続で使用するプロトコルを選択します。デフォルトでは、IPsec と L2TP over IPsec の両方が選択されています。
  - [Enable IKEv2 Protocol]：リモート アクセス接続プロファイルで使用するために IKEv2 プロトコルをイネーブルにします。これは、先ほど選択したグループ ポリシーの属性です。

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

フィールド

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

IPsec または SSL VPN 接続プロファイルへの証明書のマッピング

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

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

ポリシーに一致する証明書グループは、証明書ユーザの権限グループを特定するために使用する方法を定義します。これらの方式のいずれかまたはすべてを使用できます。

まず、[Configuration] > [Remote] [Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] で、証明書と接続プロファイルを照合するポリシーを設定します。設定するルールを選択する場合、[Rules] に移動してルールを指定します。次に、各 IPsec 接続プロファイルおよび SSL VPN 接続プロファイルの証明書ベース基準を作成する方法を示します。

上部（[Certificate to Connection Profile Maps]）に表示されるテーブルを使用して、次のいずれかを実行します。

ステップ 1　「map」というリスト名を作成し、リストのプライオリティを指定して、そのリストを接続プロファイルに割り当てます。

リストをテーブルに追加すると、ASDM で強調表示されます。

ステップ 2　証明書ベース ルールを追加する接続プロファイルにリストが割り当てられていることを確認します。

テーブルにリストを追加すると、ASDM で強調表示されます。ASDM のペインの下部のテーブルには、関連付けられたリスト エントリが表示されます。

ステップ 3　下部のテーブル（[Mapping Criteria]）を使用して、選択したリストのエントリを表示、追加、変更、または削除します。

リストの各エントリは、1 つの証明書ベース ルールで構成されています。ASA が関連付けられたマップ インデックスを選択するには、マッピング基準リストのルールすべてが証明書の内容と一致する必要があります。1 つまたは別の基準が一致する場合に接続を割り当てるには、照合基準ごとにリストを 1 つ作成します。

フィールドの詳細については、次の項を参照してください。

- 「ポリシーに一致する証明書の設定」
- 「Add/Edit Certificate Matching Rule」
- 「[Add/Edit Certificate Matching Rule Criterion]」

ポリシーに一致する証明書の設定

IPsec 接続において、ポリシーに一致する証明書グループは、証明書ユーザの権限グループを特定するために使用する方法を定義します。これらの方法のいずれかまたはすべてを使用できます。

フィールド

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

Add/Edit Certificate Matching Rule

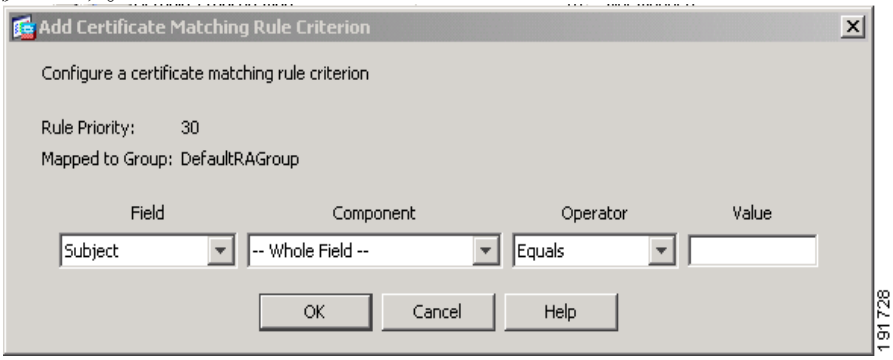
[Configuration] > [VPN] > [IKE] > [Certificate Group Matching] > [Rules] > [Add/Edit Certificate Matching Rule]

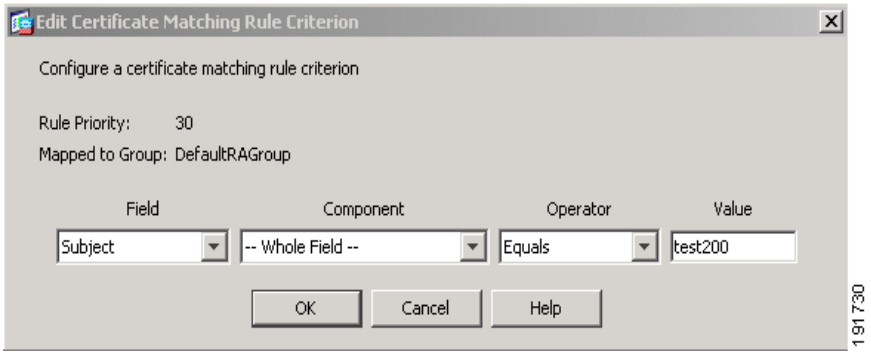
[Add/Edit Certificate Matching Rule] ダイアログボックスを使用して、接続プロファイルにリストの名前（map）を割り当てます。

フィールド

- [Map]：次のいずれかを選択します。
  - [Existing]：ルールを含めるマップの名前を選択します。
  - [New]：ルールの新しいマップ名を入力します。
- [Rule Priority]：10 進数を入力して、接続要求を受け取ったときに ASA がマップを評価する順序を指定します。定義されている最初のルールのデフォルト プライオリティは 10 です。ASA は、最低位のプライオリティ番号のマップと最初に比較して各接続を評価します。
- [Mapped to Connection Profile]：以前は「トンネル グループ」と呼んでいた接続プロファイルを選択して、このルールにマッピングします。

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





[Add/Edit Certificate Matching Rule Criterion]

[Configuration] > [VPN] > [IKE] > [Certificate Group Matching] > [Rules] > [Add/Edit Certificate Matching Rule Criterion]

[Add/Edit Certificate Matching Rule Criterion] ダイアログボックスを使用して、選択した接続プロファイルの証明書照合ルールの基準を設定します。

フィールド

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

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

- [Operator]：ルールで使用する演算子を選択します。
  - [Equals]：識別名フィールドが値に完全一致する必要があります。
  - [Contains]：識別名フィールドに値が含まれている必要があります。
  - [Does Not Equal]：識別名フィールドが値と一致しないようにします。
  - [Does Not Contain]：識別名フィールドに値が含まれないようにします。
- [Value]：255 文字までの範囲で演算子のオブジェクトを指定します。Extended Key Usage 機能の場合、ドロップダウン リストで事前定義された値のいずれかを選択するか、他の拡張の OID を入力できます。事前定義された値は次のとおりです。

選択項目	キー使用の目的	OID 文字列
clientauth	クライアント認証	1.3.6.1.5.5.7.3.2
codesigning	コード署名	1.3.6.1.5.5.7.3.3
emailprotection	安全な電子メール保護	1.3.6.1.5.5.7.3.4

選択項目	キー使用の目的	OID 文字列
clientauth	クライアント認証	1.3.6.1.5.5.7.3.2
ocspsigning	OCSP 署名	1.3.6.1.5.5.7.3.9
serverauth	サーバ認証	1.3.6.1.5.5.7.3.1
timestamping	タイム スタンプ	1.3.6.1.5.5.7.3.8

Site-to-Site 接続プロファイル

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

ASA では、IKEv1 または IKEv2 を使用して IPv4 または IPv6 の IPsec LAN-to-LAN VPN 接続がサポートされ、内部 IP ヘッダーおよび外部 IP ヘッダーを使用して内部ネットワークおよび外部ネットワークがサポートされます。

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

- [Access Interfaces]：インターフェイスのリモート ピア デバイスによってアクセスできるデバイス インターフェイスのテーブルが表示されます。
  - [Interface]：アクセスをイネーブルまたはディセーブルにするデバイス インターフェイス。
  - [Allow IKEv1 Access]：ピア デバイスによる IPsec IKEv1 アクセスをイネーブルにする場合にオンにします。
  - [Allow IKEv2 Access]：ピア デバイスによる IPsec IKEv2 アクセスをイネーブルにする場合にオンにします。
- [Connection Profiles]：プロファイルを追加、編集、または削除できる接続プロファイルのテーブルを表示します。
  - [Add]：[Add IPsec Site-to-Site connection profile] ダイアログボックスが開きます。
  - [Edit]：[Edit IPsec Site-to-Site connection profile] ダイアログボックスが開きます。
  - [Delete]：選択した接続プロファイルを削除します。確認されず、やり直しもできません。
  - [Name]：接続プロファイルの名前。
  - [Interface]：接続プロファイルがイネーブルになっているインターフェイス。
  - [Local Network]：ローカル ネットワークの IP アドレスを指定します。
  - [Remote Network]：リモート ネットワークの IP アドレスを指定します。
  - [IKEv1 Enabled]：接続プロファイルに対してイネーブルになっている IKEv1 を表示します。
  - [IKEv2 Enabled]：接続プロファイルに対してイネーブルになっている IKEv2 を表示します。
  - [Group Policy]：接続プロファイルのデフォルト グループ ポリシーを表示します。

Site-to-Site 接続プロファイルの設定

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

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

IPv4 アドレッシングと IPv6 アドレッシングが混在した、またはすべて IPv6 アドレッシングの LAN-to-LAN 接続については、両方のピアが Cisco ASA 5500 シリーズ セキュリティ アプライアンスの場合、および両方の内部ネットワークのアドレッシング方式が一致している場合（両方が IPv4 または両方が IPv6 の場合）は、セキュリティ アプライアンスで VPN トンネルがサポートされます。

具体的には、両方のピアが Cisco ASA 5500 シリーズ ASA の場合、次のトポロジがサポートされます。

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

[Basic] パネルのフィールド

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

  - [Enable IKEv1] : 指定したグループ ポリシーでキー交換プロトコル IKEv1 をイネーブルにします。
  - [Enable IKEv2] : 指定したグループ ポリシーでキー交換プロトコル IKEv2 をイネーブルにします。
- [IKEv1 Settings] タブ：IKEv1 の次の認証設定および暗号化設定を指定します。
  - [Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Device Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [IKE Policy]：IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Manage]：[Configure IKEv1 Proposals] ダイアログボックスが開きます。
  - [IPsec Proposal]：IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [IKEv2 Settings] タブ：IKEv2 の次の認証設定および暗号化設定を指定します。
  - [Local Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Local Device Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [Remote Peer Pre-shared Key] : トンネル グループのリモート ピア事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Remote Peer Certificate Authentication]：[Allowed] をオンにして、この接続プロファイルの IKEv2 接続用の証明書認証を許可します。
  - [Manage]：証明書の表示や新規証明書の追加を実行できる [Manage CA Certificates] ダイアログが開きます。
  - [IKE Policy]：IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Manage]：[Configure IKEv1 Proposals] ダイアログボックスが開きます。
  - [IPsec Proposal]：IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Select]：IKEv2 接続の接続プロファイルにプロポーザルを割り当てることができる [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開きます。
  - この接続プロファイルには、[Advanced] > [Crypto Map Entry] もあります。

Site-to-Site トンネル グループの設定

このパネルにはさまざまなパスからアクセスできます。

[Add or Edit IPsec Site-to-Site Tunnel Group] ダイアログボックスでは、追加する IPsec Site-to-Site 接続の属性を指定できます。また、IKE ピアとユーザ認証パラメータの選択、IKE キープアライブ モニタリングの設定、およびデフォルト グループ ポリシーの選択も行うことができます。

フィールド

- [Name]：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [IKE Authentication]：IKE ピアの認証で使用する事前共有キーおよび ID 証明書パラメータを指定します。
  - [Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Identity Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [IKE Peer ID Validation]：IKE ピア ID の有効性をチェックするかどうかを指定します。デフォルトは Required です。
- [IPsec Enabling]：この接続プロファイルのグループ ポリシー、およびそのポリシーで指定したキー交換プロトコルを指定します。
  - [Group Policy Name]：この接続プロファイルに関連付けられているグループ ポリシーを指定します。
  - [Manage]：[Browse Remote Network] ダイアログボックスが開きます。このダイアログボックスでは、リモート ネットワークを選択できます。
  - [Enable IKEv1] : 指定したグループ ポリシーでキー交換プロトコル IKEv1 をイネーブルにします。
  - [Enable IKEv2] : 指定したグループ ポリシーでキー交換プロトコル IKEv2 をイネーブルにします。
- [IKEv1 Settings] タブ：IKEv1 の次の認証設定および暗号化設定を指定します。
  - [Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Device Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [IKE Policy]：IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Manage]：[Configure IKEv1 Proposals] ダイアログボックスが開きます。
  - [IPsec Proposal]：IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [IKEv2 Settings] タブ：IKEv2 の次の認証設定および暗号化設定を指定します。
  - [Local Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Local Device Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [Remote Peer Pre-shared Key] : トンネル グループのリモート ピア事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。

  - [Remote Peer Certificate Authentication]：[Allowed] をオンにして、この接続プロファイルの IKEv2 接続用の証明書認証を許可します。
  - [Manage]：証明書の表示や新規証明書の追加を実行できる [Manage CA Certificates] ダイアログが開きます。
  - [IKE Policy]：IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Manage]：[Configure IKEv1 Proposals] ダイアログボックスが開きます。
  - [IPsec Proposal]：IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Select]：IKEv2 接続の接続プロファイルにプロポーザルを割り当てることができる [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開きます。
- [IKE Keepalive]：IKE キープアライブ モニタリングをイネーブルにし、設定を行います。次の属性の中から 1 つだけ選択できます。
  - [Disable Keep Alives]：IKE キープアライブをイネーブルまたはディセーブルにします。
  - [Monitor Keep Alives]：IKE キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
  - [Confidence Interval]：IKE キープアライブの信頼間隔を指定します。これは、ピアがキープアライブ モニタリングを開始するまでに ASA が許可するアイドル時間を表す秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 10 秒です。
  - [Retry Interval]：IKE キープアライブのリトライ間の待機秒数を指定します。デフォルトは 2 秒です。
  - [Head end will never initiate keepalive monitoring]：中央サイトの ASA がキープアライブ モニタリングを開始しないように指定します。

Site-to-Site 接続プロファイルでのクリプト マップ エントリの設定

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

クリプト マップのフィールド

- [Priority]：一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。
- [Perfect Forward Secrecy]：特定の IPsec SA のキーが他の秘密情報（他のキーなど）から導出されたものでないことを保証します。PFS により、攻撃者がキーを突破できたとしても、そのキーから他のキーを導出できないようにします。PFS をイネーブルにすると、Diffie-Hellman Group リストがアクティブになります。
  - [Diffie-Hellman Group]：2 つの IPsec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1（768 ビット）、Group 2（1024 ビット）、および Group 5（1536 ビット）の中から選択します。
- [Enable NAT-T]：このポリシーの NAT Traversal（NAT-T）をイネーブルにします。これにより IPsec ピアは、NAT デバイスを介してリモート アクセスと LAN-to-LAN の両方の接続を確立できます。

- [Enable Reverse Route Injection]：リモート トンネルのエンドポイントによって保護されているネットワークとホストのルーティング プロセスに、スタティック ルートが自動的に挿入されるようにすることができます。
- [Security Association Lifetime]：セキュリティ アソシエーション（SA）の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
  - [Time]：時（hh）、分（mm）、および秒（ss）単位で SA のライフタイムを指定します。
  - [Traffic Volume]：キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロード データのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。

Crypto Map Entry for Static Peer Address

このダイアログボックスでは、ピアの IP アドレスがスタティック アドレスである場合に、接続プロファイルの暗号パラメータを指定します。

フィールド

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

- [Connection Type]：許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。
- [Send ID Cert.Chain]：証明書チェーン全体の送信をイネーブルにします。
- [IKE Negotiation Mode]：SA、Main、または Aggressive の中から、セットアップでキー情報を交換するときのモードを設定します。ネゴシエーションの発信側が使用するモードも設定されます。応答側は自動ネゴシエーションします。Aggressive モードは高速で、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。Main モードは低速で、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。このモードはより安全性が高く、デフォルトで選択されています。[Aggressive] を選択すると、[Diffie-Hellman Group] リストがアクティブになります。
- [Diffie-Hellman Group]：2 つの IPsec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1（768 ビット）、Group 2（1024 ビット）、および Group 5（1536 ビット）の中から選択します。

CA 証明書の管理

[IKE Peer Authentication] の下にある [Manage] をクリックすると、[Manage CA Certificates] ダイアログボックスが開きます。このダイアログボックスを使用して、IKE ピア認証で使用可能な CA 証明書のリストのエントリを、表示、追加、編集、および削除します。

[Manage CA Certificates] ダイアログボックスには、証明書の発行先、証明書の発行元、証明書の有効期限、および利用データなど、現在設定されている証明書の情報が一覧表示されます。

フィールド

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

[Install Certificate]

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

- 証明書ファイルを参照してファイルからインストールします。
- 事前取得済みの PEM 形式の証明書テキストをこのダイアログボックスのボックスに貼り付けます。
- [Use SCEP]：Simple Certificate Enrollment Protocol（SCEP）の使用を指定します。証明書サービスのアドオンは、Windows Server 2003 ファミリで実行されます。SCEP プロトコルのサポートを提供し、これによりシスコのルータおよび他の中間ネットワーク デバイスは、証明書を取得できます。
  - [SCEP URL: http://]：SCEP 情報のダウンロード元の URL を指定します。
  - [Retry Period]：SCEP クエリー間の必須経過時間を分数で指定します。
  - [Retry Count]：リトライの最大許容回数を指定します。
- [More Options]：[Configure Options for CA Certificate] ダイアログボックスが開きます。

[Configure Options for CA Certificate]

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

[Revocation Check] ダイアログボックス

このダイアログボックスを使用して、CA 証明書の失効チェックについての情報を指定します。

フィールド

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

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

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

フィールド

- [Strip the realm from the username before passing it on to the AAA server] : レルム（管理ドメイン）をユーザ名から除去してから、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザ名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@example.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザ名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注） レルムとグループは、両方をユーザ名に追加できます。その場合、ASA は、グループと AAA 機能用のレルムに対して設定されたパラメータを使用します。このオプションのフォーマットは *JaneDoe@example.com#VPNGroup* のように、*ユーザ名[@realm][<# または !>グループ]* という形式を取ります。このオプションを選択した場合は、グループ デリミタとして # または !を使用する必要があります。これは、@ がレルム デリミタとしても使用されている場合には、ASA が @ をグループ デリミタと解釈できないためです。

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

VPN 3000 Concentrator は user@grouppolicy をサポートしていますが、ASA は user@grouppolicy をサポートしていません。L2TP/IPsec クライアントだけが、user@tunnelgroup を介したトンネル スイッチングをサポートしています。

- [Strip the group from the username before passing it on to the AAA server]：グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、ASA は、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、*ユーザ名<デリミタ>グループ*の形式でグループをユーザ名に追加します。
- [Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注） override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

  - [Enable notification upon password expiration to allow user to change password]: このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザに通知するか、またはパスワードが期限切れになる当日にユーザに通知するかを選択できます。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ～ 180 日です。

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

    どちらの場合でも、変更されずにパスワードが期限切れになると、ASA はパスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

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

    この機能では、MS-CHAPv2 を使用する必要があります。

[Add/Edit Connection Profile] > [General] > [Authentication]

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

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

[Add/Edit SSL VPN Connection] > [General] > [Authorization]

このダイアログボックスでの設定は、ASA 全体の接続（トンネル グループ）にグローバルに適用されます。このダイアログボックスでは、次の属性を設定できます。

- [Authorization Server Group]：LOCAL グループを含む、利用可能な認可サーバ グループを一覧表示します。None（デフォルト）も選択可能です。None 以外を選択すると、[Users must exist in authorization database to connect] チェックボックスが利用できるようになります。
- [Users must exist in authorization database to connect]：ASA に対し、認可データベース内のユーザだけに接続を許可するように命令します。デフォルトでは、この機能はディセーブルになっています。認可サーバでこの機能を使用するように設定しておく必要があります。
- [Interface-Specific Authorization Server Groups]：（オプション）インターフェイスごとに認可サーバ グループを設定できます。インターフェイスに固有の認可サーバ グループは、グローバル サーバ グループよりも優先されます。インターフェイスに固有の認可を明示的に設定していない場合には、グループ レベルでだけ認可が実行されます。
  - [Interface]：認可を実行するインターフェイスを選択します。標準のインターフェイスは、outside（デフォルト）、inside、および DMZ です。他のインターフェイスを設定した場合には、そのインターフェイスもリストに表示されます。
  - [Server Group]：LOCAL グループを含む、先に設定した利用可能な認可サーバ グループを選択します。サーバ グループは、複数のインターフェイスと関連付けることができます。
  - [Add]：[Add] をクリックすると、インターフェイスまたはサーバ グループ設定がテーブルに追加され、利用可能なリストからインターフェイスが削除されます。
  - [Remove]：[Remove] をクリックすると、インターフェイスまたはサーバ グループがテーブルから削除され、利用可能なリストにインターフェイスが戻ります。
- [Authorization Settings]：ASA が認可のために認識するユーザ名の値を設定できるようにします。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 認可を必要とするユーザに適用されます。
  - [Use entire DN as username]：認定者名（DN）全体をユーザ名として使用することを許可します。
  - [Specify individual DN fields as the username]：個々の DN フィールドをユーザ名として使用することをイネーブルにします。
  - [Primary DN Field]：選択内容の DN フィールド識別子すべてを一覧表示します。

DN フィールド	定義
Country（C）	2 文字の国名略記。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	人やシステム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有する人、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、III などの世代修飾子。
Given Name（GN）	証明書所有者の名。
Initials（I）	証明書所有者の姓と名の最初の文字。

DN フィールド	定義
Locality（L）	組織が所在する市または町。
Name（N）	証明書所有者の名。
Organization（O）	会社、施設、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	博士など、証明書の所有者の肩書。
User ID（UID）	証明書の所有者の識別番号。
User Principal Name（UPN）	スマート カードによる証明書認証で使用。

  - [Secondary DN Field]：選択内容の DN フィールド識別子のすべて（上記の表を参照）を一覧表示し、選択していない場合には None オプションを追加します。

[Add/Edit Tunnel Group] > [General] > [Client Address Assignment]

アドレス割り当てに DHCP またはアドレス プールを使用するかどうかを指定するには、[Configuration] > [VPN] > [I P Address Management] > [Assignment] に移動します。[Add or Edit Tunnel Group] ダイアログボックス > [General] > [Client Address Assignment] ダイアログボックスでは、次の Client Address Assignment 属性を設定できます。

- [DHCP Servers]：使用する DHCP サーバを指定します。一度に最大 10 台のサーバを追加できます。
  - [IP Address]：DHCP サーバの IP アドレスを指定します。
  - [Add]：指定された DHCP サーバを、クライアント アドレス割り当て用のリストに追加します。
  - [Delete]：指定された DHCP サーバを、クライアント アドレス割り当て用のリストから削除します。確認されず、やり直しもできません。
- [Address Pools]：次のパラメータを使用して、最大 6 つのアドレス プールを指定できます。
  - [Available Pools]：選択可能な設定済みのアドレス プールを一覧表示します。
  - [Add]：選択したアドレス プールをクライアント アドレス割り当て用のリストに追加します。
  - [Remove]：選択したアドレス プールを [Assigned Pools] リストから [Available Pools] リストに移動します。
  - [Assigned Pools]：アドレス割り当て用に選択したアドレス プールを一覧表示します。

（注） インターフェイスに固有のアドレス プールを設定するには、[Advanced] をクリックします。

[Add/Edit Tunnel Group] > [General] > [Advanced]

[Add or Edit Tunnel Group] ダイアログボックスの [General] の [Advanced] ダイアログボックスでは、インターフェイスに固有の次の属性を設定できます。

- [Interface-Specific Authentication Server Groups]：インターフェイスとサーバ グループを認証用に設定できます。
  - [Interface]：選択可能なインターフェイスを一覧表示します。
  - [Server Group]：このインターフェイスで利用可能な認証サーバ グループを一覧表示します。
  - [Use LOCAL if server group fails]：サーバ グループに障害が発生した場合の LOCAL データベースへのフォールバックをイネーブルまたはディセーブルにします。
  - [Add]：選択した利用可能なインターフェイスと認証サーバ グループ間のアソシエーションを、割り当てられたリストに追加します。
  - [Remove]：選択したインターフェイスと認証サーバ グループのアソシエーションを、割り当てられたリストから利用可能なリストに移動します。
  - [Interface/Server Group/Use Fallback]：割り当てられたリストに追加した選択内容を表示します。
- [Interface-Specific Client IP Address Pools] : インターフェイスとクライアントの IP アドレス プールを指定できます。最大 6 個のプールを指定できます。
  - [Interface]：追加可能なインターフェイスを一覧表示します。
  - [Address Pool]：このインターフェイスと関連付けできるアドレス プールを一覧表示します。
  - [Add]：選択した利用可能なインターフェイスとクライアントの IP アドレス プール間のアソシエーションを、割り当てられたリストに追加します。
  - [Remove]：選択したインターフェイスまたはアドレス プールのアソシエーションを、割り当てられたリストから利用可能なリストに移動します。
  - [Interface/Address Pool]：割り当てられたリストに追加された選択内容を表示します。

[Add/Edit Tunnel Group] > [IPsec for Remote Access] > [IPsec]

[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add/Edit Tunnel Group] > [IPSec for Remote Access] > [IPSec] タブ

[IPsec for Remote Access] の [Add or Edit Tunnel Group] ダイアログボックスにある [IPsec] ダイアログボックスでは、IPsec に固有のトンネル グループ パラメータを設定または編集できます。

フィールド

- [Pre-shared Key]：トンネル グループの事前共有キーの値を指定できます。事前共有キーの最大長は 128 文字です。
- [Trustpoint Name]：トラストポイントが設定されている場合には、トラストポイント名を選択します。トラストポイントとは、認証局を表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。
- [Authentication Mode]：認証モードを、none、xauth、または hybrid の中から指定します。
  - [none]：認証モードを指定しません。

- [xauth]：IKE 拡張認証モードを使用するように指定します。この認証モードは、TACACS+ または RADIUS を使用する IKE 内のユーザを認証する機能を提供します。
- [hybrid]：ハイブリッド モードを使用するように指定します。この認証モードでは、セキュリティ アプライアンス認証にデジタル認証を使用でき、リモート VPN ユーザ認証に別のレガシー方式（RADIUS、TACACS+、SecurID など）を使用できます。このモードでは、インターネット キー交換（IKE）のフェーズ 1 が次の手順に分かれています。これらを合せてハイブリッド認証と呼びます。

1. セキュリティ アプライアンスでは、リモート VPN ユーザが標準公開キー技術で認証されます。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
2. 次に、拡張認証（xauth）交換でリモート VPN ユーザが認証されます。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注） 認証タイプをハイブリッドに設定する前に、認証サーバを設定し、事前共有キーを作成する必要があります。

- [IKE Peer ID Validation]：IKE ピア ID 確認要求を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- [Enable sending certificate chain]：証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [ISAKMP Keep Alive]：ISAKMP キープアライブ モニタリングをイネーブルにし、設定します。
  - [Disable Keep Alives]：ISAKMP キープアライブをイネーブルまたはディセーブルにします。
  - [Monitor Keep Alives]：ISAKMP キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
  - [Confidence Interval]：ISAKMP キープアライブの信頼間隔を指定します。これは、ピアがキープアライブ モニタリングを開始するまでに ASA が許可するアイドル時間を表す秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 300 秒です。
  - [Retry Interval]：ISAKMP キープアライブのリトライ間の待機秒数を指定します。デフォルトは 2 秒です。
  - [Head end will never initiate keepalive monitoring]：中央サイトの ASA がキープアライブ モニタリングを開始しないように指定します。
- [Interface-Specific Authentication Mode]：認証モードをインターフェイスごとに指定します。
  - [Interface]：名前付きインターフェイスを選択します。デフォルトのインターフェイスは inside と outside ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
  - [Authentication Mode]：認証モードを、上記の none、xauth、または hybrid の中から選択できます。
  - [Interface/Authentication Mode] テーブル：インターフェイス名と、選択されている関連認証モードを表示します。
  - [Add]：選択したインターフェイスと認証モードのペアを [Interface/Authentication Modes] テーブルに追加します。
  - [Remove]：選択したインターフェイスと認証モードのペアを [Interface/Authentication Modes] テーブルから削除します。

- [Client VPN Software Update Table]：クライアント タイプ、VPN クライアントのリビジョン、およびインストールされている各クライアント VPN ソフトウェア パッケージのイメージ URL を一覧表示します。クライアント タイプごとに、許可されるクライアント ソフトウェア リビジョンと、必要に応じて、ソフトウェア アップグレードをダウンロードする URL または IP アドレスを指定できます。クライアント アップデート メカニズム（[Client Update] ダイアログボックスに詳細説明があります）は、この情報を使用して、各 VPN クライアントが適切なリビジョン レベルで実行されているかどうか、適切であれば、通知メッセージとアップデート メカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。
  - [Client Type]：VPN クライアント タイプを識別します。
  - [VPN Client Revisions]：許可される VPN クライアントのリビジョン レベルを指定します。
  - [Image URL]：適切な VPN クライアント ソフトウェア イメージをダウンロードできる URL または IP アドレスを指定します。ダイアログボックスベースの VPN クライアントの場合、URL は http:// または https:// という形式です。クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアントの場合、URL は tftp:// という形式です。

Site-to-Site VPN のトンネル グループの追加および編集

[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add/Edit Tunnel Group] > [IPSec for Remote Access] > [IPSec] タブ

[Add or Edit Tunnel Group] ダイアログボックスでは、この Site-to-Site 接続プロファイルのトンネル グループ パラメータを設定または編集できます。

フィールド

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

- [Default Group Policy]：次のグループ ポリシーの属性を指定します。
  - [Group Policy]：デフォルトのグループ ポリシーとして使用するグループ ポリシーを選択します。デフォルト値は DfltGrpPolicy です。
  - [Manage]：[Configure Group Policies] ダイアログボックスが開きます。
  - [IPsec Protocol]：この接続プロファイルでの IPsec プロトコルの使用をイネーブルまたはディセーブルにします。

[Add/Edit Tunnel Group] > [IPsec for LAN to LAN Access] > [General] > [Basic]

[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add/Edit Tunnel Group] > [IPSec for LAN to LAN Access] > [General] タブ > [Basic] タブ

Site-to-Site リモート アクセスの [Add or Edit Tunnel Group] ダイアログボックスにある、[General] タブの [Basic] ダイアログボックスでは、追加するトンネル グループの名前を指定し（Add 機能だけ）、グループ ポリシーを選択できます。

[Edit Tunnel Group] ダイアログボックスの [General] ダイアログボックスには、変更するトンネル グループの名前とタイプが表示されます。

フィールド

- [Name]：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [Type]：（*表示専用*）追加または編集するトンネル グループのタイプを表示します。このフィールドの内容は、前のダイアログボックスでの選択内容によって異なります。
- [Group Policy]：現在設定されているグループ ポリシーを一覧表示します。デフォルト値は、デフォルト グループ ポリシーである DfltGrpPolicy です。
- [Strip the realm (administrative domain) from the username before passing it on to the AAA server]：レルムをユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザ名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@example.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザ名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注） レルムとグループは、両方をユーザ名に追加できます。その場合、ASA は、グループと AAA 機能用のレルムに対して設定されたパラメータを使用します。このオプションのフォーマットは *JaneDoe@example.com#VPNGroup* のように、*ユーザ名[@realm][<# または !>グループ]* という形式を取ります。このオプションを選択した場合は、グループ デリミタとして # または !を使用する必要があります。これは、@ がレルム デリミタとしても使用されている場合には、ASA が @ をグループ デリミタと解釈できないためです。

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

VPN 3000 Concentrator は user@grouppolicy をサポートしていますが、ASA は user@grouppolicy をサポートしていません。L2TP/IPsec クライアントだけが、user@tunnelgroup を介したトンネル スイッチングをサポートしています。

- [Strip the group from the username before passing it on to the AAA server]: グループ名をユーザ名から除去し、そのユーザ名を AAA サーバに渡す処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、ASA は、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および！で、@ が Group Lookup のデフォルトです。*JaneDoe@VPNGroup*、*JaneDoe#VPNGroup* や *JaneDoe!VPNGroup* のように、*ユーザ名<デリミタ>グループ*の形式でグループをユーザ名に追加します。
- [Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

  - [Enable notification upon password expiration to allow user to change password]: このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。[Enable notification prior to expiration] チェックボックスをオンにしないと、ユーザは、パスワードの期限が切れた後で通知を受信します。
  - [Enable notification prior to expiration]：このオプションをオンにすると、ASA は、リモート ユーザのログイン時に、現在のパスワードの期限切れが迫っているか、期限が切れていることを通知し、パスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

    この処理によってパスワードの期限が切れるまでの日数が変わるわけではなく、通知がイネーブルになるということに注意してください。このチェックボックスをオンにしたら、日数も指定する必要があります。
  - [Notify...days prior to expiration]：現在のパスワードの期限切れが迫っていることをユーザに通知する日を、期限切れになるまでの日数で指定します。範囲は 1 ～ 180 日です。

[Add/Edit Tunnel Group] > [IPsec for LAN to LAN Access] > [IPsec]

[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add/Edit Tunnel Group] > [IPSec for LAN to LAN Access] > [IPSec] タブ

Site-to-Site アクセス用 IPsec の [Add or Edit Tunnel Group] ダイアログボックスの [IPsec] ダイアログボックスでは、IPsec Site-to-Site に固有のトンネル グループ パラメータを設定または編集できます。

フィールド

- [Name]：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [Type]：（*表示専用*）追加または編集するトンネル グループのタイプを表示します。このフィールドの内容は、前のダイアログボックスでの選択内容によって異なります。

- [Pre-shared Key]：トンネル グループの事前共有キーの値を指定できます。事前共有キーの最大長は 128 文字です。
- [Trustpoint Name]：トラストポイントが設定されている場合には、トラストポイント名を選択します。トラストポイントとは、認証局を表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。
- [Authentication Mode]：認証モードを、none、xauth、または hybrid の中から指定します。
  - [none]：認証モードを指定しません。
  - [xauth]：IKE 拡張認証モードを使用するように指定します。この認証モードは、TACACS+ または RADIUS を使用する IKE 内のユーザを認証する機能を提供します。
  - [hybrid]：ハイブリッド モードを使用するように指定します。この認証モードでは、セキュリティ アプライアンス認証にデジタル認証を使用でき、リモート VPN ユーザ認証に別のレガシー方式（RADIUS、TACACS+、SecurID など）を使用できます。このモードでは、インターネット キー交換（IKE）のフェーズ 1 が次の手順に分かれています。これらを合せてハイブリッド認証と呼びます。

    1. セキュリティ アプライアンスでは、リモート VPN ユーザが標準公開キー技術で認証されます。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
    2. 次に、拡張認証（xauth）交換でリモート VPN ユーザが認証されます。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注） 認証タイプをハイブリッドに設定する前に、認証サーバを設定し、事前共有キーを作成する必要があります。

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

- [Interface-Specific Authentication Mode]：認証モードをインターフェイスごとに指定します。
  - [Interface]：名前付きインターフェイスを選択します。デフォルトのインターフェイスは inside と outside ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
  - [Authentication Mode]：認証モードを、上記の none、xauth、または hybrid の中から選択できます。
  - [Interface/Authentication Mode] テーブル：インターフェイス名と、選択されている関連認証モードを表示します。
  - [Add]：選択したインターフェイスと認証モードのペアを [Interface/Authentication Modes] テーブルに追加します。
  - [Remove]：選択したインターフェイスと認証モードのペアを [Interface/Authentication Modes] テーブルから削除します。
- [Client VPN Software Update Table]：クライアント タイプ、VPN クライアントのリビジョン、およびインストールされている各クライアント VPN ソフトウェア パッケージのイメージ URL を一覧表示します。クライアント タイプごとに、許可されるクライアント ソフトウェア リビジョンと、必要に応じて、ソフトウェア アップグレードをダウンロードする URL または IP アドレスを指定できます。クライアント アップデート メカニズム（[Client Update] ダイアログボックスに詳細説明があります）は、この情報を使用して、各 VPN クライアントが適切なリビジョン レベルで実行されているかどうか、適切であれば、通知メッセージとアップデート メカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。
  - [Client Type]：VPN クライアント タイプを識別します。
  - [VPN Client Revisions]：許可される VPN クライアントのリビジョン レベルを指定します。
  - [Image URL]：適切な VPN クライアント ソフトウェア イメージをダウンロードできる URL または IP アドレスを指定します。Windows ベースの VPN クライアントの場合、URL は http:// または https:// という形式です。クライアント モードの ASA 5505 または VPN 3002 ハードウェア クライアントの場合、URL は tftp:// という形式です。

[Clientless SSL VPN Access] > [Connection Profiles] > [Add/Edit] > [General] > [Basic]

[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add/Edit] > [WebVPN Access] > [General] タブ > [Basic] タブ

[Add or Edit] ペインの [General] タブの [Basic] ダイアログボックスでは、追加するトンネル グループの名前の指定、グループ ポリシーの選択、およびパスワード管理の設定を行うことができます。

[Edit Tunnel Group] ダイアログボックスの [General] ダイアログボックスには、選択したトンネル グループの名前とタイプが表示されます。その他の機能は、[Add Tunnel Group] ダイアログボックスと同じです。

フィールド

- [Name]：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [Type]：追加または削除するトンネル グループのタイプを表示します。Edit の場合、このフィールドは表示専用で、その内容は、[Add] ダイアログボックスでの選択内容によって異なります。
- [Group Policy]：現在設定されているグループ ポリシーを一覧表示します。デフォルト値は、デフォルト グループ ポリシーである DfltGrpPolicy です。

- [Strip the realm]：クライアントレス SSL VPN では使用できません。
- [Strip the group]：クライアントレス SSL VPN では使用できません。
- [Password Management]：AAA サーバからの account-disabled インジケータの上書きと、ユーザに対するパスワード期限切れの通知に関するパラメータを設定できます。
  - [Override account-disabled indication from AAA server]：AAA サーバからの account-disabled インジケータを上書きします。

（注）　override account-disabled を許可することは、潜在的なセキュリティ リスクとなります。

  - [Enable notification upon password expiration to allow user to change password]: このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。[Enable notification prior to expiration] チェックボックスをオンにしないと、ユーザは、パスワードの期限が切れた後で通知を受信します。
  - [Enable notification prior to expiration]：このオプションをオンにすると、ASA は、リモート ユーザのログイン時に、現在のパスワードの期限切れが迫っているか、期限が切れていることを通知し、パスワードを変更する機会をユーザに提供します。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

    この処理によってパスワードの期限が切れるまでの日数が変わるわけではなく、通知がイネーブルになるということに注意してください。このチェックボックスをオンにしたら、日数も指定する必要があります。
  - [Notify...days prior to expiration]：現在のパスワードの期限切れが迫っていることをユーザに通知する日を、期限切れになるまでの日数で指定します。範囲は 1 ～ 180 日です。

[Configuring Client Addressing for SSL VPN Connections]

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

フィールド

- [Interface-Specific IPv4 Address Pools]：設定されているインターフェイス固有のアドレス プールの一覧を表示します。
- [Interface-Specific IPv6 Address Pools]：設定されているインターフェイス固有のアドレス プールの一覧を表示します。
- [Add]：[Assign Address Pools to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスおよび割り当てるアドレス プールを選択できます。
- [Edit]：インターフェイスとアドレス プールのフィールドに値が取り込まれた状態で、[Assign Address Pools to Interface] ダイアログボックスが開きます。
- [Delete]：選択したインターフェイスに固有のアドレス プールを削除します。確認されず、やり直しもできません。

[Assign Address Pools to Interface]

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

フィールド

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

[Select Address Pools]

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

フィールド

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

[Add or Edit an IP Address Pool]

IP アドレス プールを設定または変更します。

フィールド

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

SSL VPN 接続の認証

[SSL VPN Connections] > [Advanced] > [Authentication] ダイアログでは、SSL VPN 接続の認証属性を設定できます。

[System Options]

このパネルには、次のパスを順に進むことによって到達できます。

- [Configuration] > [Site-to-Site VPN] > [Advanced] > [System Options]
- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [System Options]

[System Options] ペインでは、ASA での VPN セッションに固有の機能を設定できます。

フィールド

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

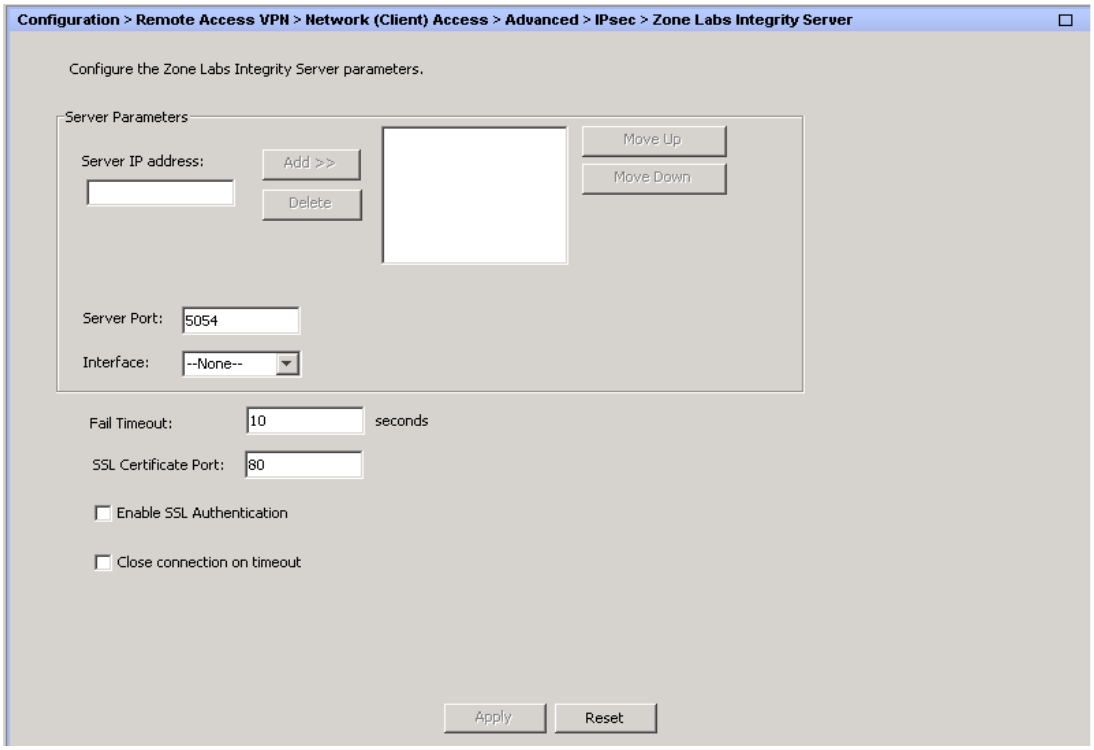
  （注） トンネル TCP フローはドロップされないため、クリーンアップは TCP タイムアウトに依存します。ただし、特定のトンネル フローのタイムアウトがディセーブルになっている場合、手動または他の方法（ピアからの TCP RST など）によってクリアされるまで、そのフローはシステム内で保持されます。

- [IPsec Security Association Lifetime]：セキュリティ アソシエーション（SA）の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
  - [Time]：時（hh）、分（mm）、および秒（ss）単位で SA のライフタイムを指定します。
  - [Traffic Volume]：キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロード データのキロバイト数を入力します。または [unlimited] をオンにします。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。
- [Enable PMTU (Path Maximum Transmission Unit) Aging] : 管理者が PMTU のエージングをイネーブルにすることができます。
  - [Interval to Reset PMTU of an SA (Security Association)] : PMTU 値が元の値にリセットされる秒数を入力します。

[Zone Labs Integrity Server]

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Zone Labs Integrity Server]

[Zone Labs Integrity Server] パネルでは、Zone Labs Integrity Server をサポートするように ASA を設定できます。このサーバは、プライベート ネットワークにアクセスするリモート クライアントでセキュリティ ポリシーを適用する目的で設計された Integrity System というシステムの一部です。本質的には、ASA が、ファイアウォール サーバに対するクライアント PC のプロキシとして機能し、Integrity クライアントと Integrity サーバ間で必要なすべての Integrity 情報をリレーします。



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

フィールド

- [Server IP address]：Integrity Server の IP アドレスを入力します。ドット付き 10 進数を使用します。
- [Add]：新しいサーバ IP アドレスを Integrity Server のリストに追加します。このボタンは、Server IP アドレス フィールドにアドレスが入力されるとアクティブになります。
- [Delete]：選択したサーバを Integrity Server リストから削除します。

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

AnyConnect 3.1 の AnyConnect Essentials

AnyConnect Essentials は別個にライセンスされた SSL VPN クライアントで、ASA 全体で設定されており、次を除いて、完全な AnyConnect 機能を提供しています。

- CSD を使用できない（HostScan/Vault/Cache Cleaner を含む）
- クライアントレス SSL VPN 非対応
- オプションの Windows Mobile のサポート（Windows Mobile ライセンスの AnyConnect が必要です）

AnyConnect Essentials クライアントは、Microsoft Windows Vista、Windows Mobile、Windows XP、Windows 2000、Linux、または Macintosh OS X を実行しているリモート エンド ユーザに Cisco SSL VPN Client の利点をもたらします。

AnyConnect Essentials をイネーブルにするには、[AnyConnect Essentials] ペインの [Enable AnyConnect Essentials] チェックボックスをオンにします。このペインは AnyConnect Essentials ライセンスが ASA にインストールされている場合にだけ表示されます。

AnyConnect Essentials がイネーブルされると、AnyConnect クライアントは Essentials モードを使用し、クライアントレス SSL VPN アクセスがディセーブルされます。AnyConnect Essentials がディセーブルされると、AnyConnect クライアントは完全な AnyConnect SSL VPN Client を使用します。

（注）　[Configuration] > [Device Management] > [Licensing] > [Activation Key pane simply] の AnyConnect Essentials ライセンスに関するステータス情報には、AnyConnect Essential ライセンスがインストールされているかどうかが反映されます。[Enable AnyConnect Essentials License] チェックボックスの設定はこのステータスに反映されません。

デバイスへのアクティブなクライアントレス セッションがある場合、AnyConnect Essentials モードをイネーブルにできません。SSL VPN セッションの詳細を表示するには、[SSL VPN Sessions] セクションの [Monitoring] > [VPN] > [VPN Sessions] リンクをクリックします。[Monitoring] > [VPN] > [VPN] > [VPN Statistics] > [Sessions] ペインが開きます。セッションの詳細を表示するには、[Filter By: Clientless SSL VPN] を選択して [Filter] をクリックします。セッションの詳細が表示されます。

セッションの詳細は表示せず、現在アクティブな SSL VPN セッションの数を表示するには、[Check Number of Clientless SSL Sessions] をオンにします。SSL VPN セッションの数が 0 の場合、AnyConnect Essential をイネーブルにできます。

（注）　AnyConnect Essential がイネーブルになっている場合、Secure Desktop は機能しません。ただし、Secure Desktop をイネーブルにする場合は AnyConnect Essential をディセーブルにできます。

DTLS 設定

Datagram Transport Layer Security（DTLS）をイネーブルにすることにより、SSL VPN 接続を確立する AnyConnect VPN クライアントは、SSL トンネルおよび DTLS トンネルという 2 つの同時トンネルを使用できます。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

DTLS をイネーブルにしない場合、SSL VPN 接続を確立する AnyConnect クライアント ユーザは、SSL VPN トンネルでだけ接続します。

フィールド

- [Interface]：ASA のインターフェイスのリストを表示します。
- [DTLS Enabled]：インターフェイスで AnyConnect クライアントによる DTLS 接続をイネーブルにする場合にオンにします。
- [UDP Port (default 443)]：（オプション）DTLS 接続用に別の UDP ポートを指定します。

AnyConnect VPN クライアント イメージ

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

このペインには、ASDM で設定された AnyConnect クライアント イメージが一覧表示されます。

フィールド

- [AnyConnect Client Image] テーブル：ASDM で設定されたパッケージ ファイルを表示します。ASA がイメージをリモート PC にダウンロードする順序を設定できます。
  - [Add]：[Add AnyConnect Client Image] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュ メモリ内のファイルをクライアント イメージ ファイルとして指定したり、フラッシュ メモリから、クライアント イメージとして指定するファイルを参照したりできます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - [Replace]：[Replace AnyConnect Client Image] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュ メモリ内のファイルをクライアント イメージとして指定して、[SSL VPN Client Image] テーブルで選択したイメージと置換できます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - [Delete]：テーブルからイメージを削除します。イメージを削除しても、パッケージ ファイルはフラッシュから削除されません。
  - [Move Up] および [Move Down]：上矢印と下矢印を使用して、ASA がクライアント イメージをリモート PC にダウンロードするときの順序を変更します。テーブルの一番上にあるイメージを最初にダウンロードします。このため、最もよく使用するオペレーティング システムで使用されるイメージを一番上に移動する必要があります。

[Add/Replace AnyConnect VPN Client Image]

このペインでは、AnyConnect クライアント イメージとして追加するか、またはテーブルのリストにすでに含まれているイメージと置換する、ASA フラッシュ メモリのファイルの名前を指定できます。また、識別するファイルをフラッシュ メモリから参照したり、ローカル コンピュータからファイルをアップロードしたりすることもできます。

フィールド

- [Flash SVC Image]：SSL VPN クライアント イメージとして識別する、フラッシュ メモリ内のファイルを指定します。
- [Browse Flash]：フラッシュ メモリに格納されているすべてのファイルを参照できる [Browse Flash Dialog] ダイアログボックスを表示します。
- [Upload]：[Upload Image] ダイアログボックスが表示されます。このダイアログボックスでは、クライアント イメージとして指定するファイルをローカル PC からアップロードできます。
- [Regular expression to match user-agent]：ASA が、ブラウザによって渡された User-Agent 文字列に一致させる文字列を指定します。モバイル ユーザの場合、この機能を使用してモバイル デバイスの接続時間を短縮できます。ブラウザが ASA に接続するとき、User-Agent ストリングが HTTP ヘッダーに含められます。ASA によってストリングが受信され、そのストリングがあるイメージ用に設定された式と一致すると、そのイメージがただちにダウンロードされます。この場合、他のクライアント イメージはテストされません。

[Upload Image]

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

フィールド

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

インターフェイス ACL のバイパス

このチェックボックスをオフにすることにより、アクセス ルールをローカル IP アドレスに適用することを強制的に適用できます。アクセス ルールはローカル IP アドレスに適用され、VPN パケットが復号化される前に使用されていた元のクライアント IP アドレスには適用されません。

- [Enable inbound IPSec sessions to bypass interface access-lists.Group policy and per-user authorization ACLs still apply to the traffic]：ASA は、VPN トラフィックが ASA インターフェイスで終了することをデフォルトで許可しているため、IKE または ESP（またはその他のタイプの VPN パケット）をアクセス ルールで許可する必要はありません。このチェックボックスをオンにしている場合は、復号化された VPN パケットのローカル IP アドレスに対するアクセス ルールは不要です。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、コンフィギュレーションが簡略化され、ASA のパフォーマンスはセキュリティ リスクを負うことなく最大化されます（グループ ポリシーおよびユーザ単位の許可 ACL は、引き続きトラフィックに適用されます）。

AnyConnect ホスト スキャン イメージ

[Configuration] > [Remote Access VPN] > [Host Scan Image]

AnyConnect ポスチャ モジュールにより、AnyConnect セキュア モビリティ クライアントはホストにインストールされているオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを識別できます。この情報は、ホスト スキャン アプリケーションによって収集されます。

ホスト スキャン サポート表には、ポスチャ ポリシーで使用するアンチウイルス、アンチスパイウェア、およびファイアウォール アプリケーションの製品名とバージョン情報が含まれます。シスコでは、ホスト スキャン パッケージにホスト スキャン、ホスト スキャン サポート表、および他のコンポーネントを含めて提供しています。

この章の内容は、次のとおりです。

- 「ホスト スキャンの依存関係およびシステム要件」（P.3-106）
- 「ホスト スキャン パッケージ」（P.3-107）
- 「ASA 上でのホスト スキャンのインストールと有効化」（P.3-107）
- 「ホスト スキャンに関するその他の重要なマニュアル」（P.3-111）

ホスト スキャンの依存関係およびシステム要件

AnyConnect セキュア モビリティ クライアントをポスチャ モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

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

- SCEP 認証
- AnyConnect テレメトリ モジュール

システム要件

ポスチャ モジュールは、次のいずれかのプラットフォームにインストールできます。

- Windows XP（x86 版、および x64 環境で動作する x86 版）
- Windows Vista（x86 版、および x64 環境で動作する x86 版）
- Windows 7（x86 版、および x64 環境で動作する x86 版）
- Mac OS X 10.5、10.6（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Linux（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Windows Mobile

ライセンス

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

- 基本ホスト スキャン用の AnyConnect Premium。
- 次の場合は、Advanced Endpoint Assessment ライセンスが必要です。
  - 修復
  - モバイル デバイス管理

Advanced Endpoint Assessment をサポートするためのアクティベーション キーの入力

Advanced Endpoint Assessment には、Endpoint Assessment 機能のすべてが含まれており、バージョン要件を満たすために非準拠のコンピュータのアップデートを試行するように設定できます。次の手順に従い、Advanced Endpoint Assessment をサポートするために、シスコからキーを取得したら、ASDM を使用してキーのアクティベーションを行います。

ステップ 1　[Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択します。

ステップ 2　[New Activation Key] フィールドにキーを入力します。

ステップ 3　[Update Activation Key] をクリックします。

ステップ 4　[File] > [Save Running Configuration to Flash] を選択します。

[Advanced Endpoint Assessment] エントリが表示され、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] ペインの [Host Scan Extensions] 領域内の [Configure] ボタンがアクティブになります。[Host Scan] ペインは、CSD が有効になっている場合に限りアクセスできます。

ホスト スキャン パッケージ

ASA へのホスト スキャン パッケージは次のいずれかの方法でロードできます。

- **hostscan-*version*.pkg** は、スタンドアロン パッケージとしてアップロードできます。
- **anyconnect-win-*version*-k9.pkg** は、AnyConnect Secure Mobility パッケージをアップロードすることによって、アップロードできます。
- **csd_version-k9.pkg** は、Cisco Secure Desktop をアップロードすることによって、アップロードできます。

ファイル	説明
hostscan-*version*.pkg	このファイルには、ホスト スキャン ソフトウェア、ホスト スキャン ライブラリ、およびサポート表が含まれています。
anyconnect-NGC-win-*version*-k9.pkg	このパッケージには、hostscan-*version*.pkg ファイルなど、Cisco AnyConnect セキュア モビリティ クライアントのすべての機能が含まれています。
csd_*version*-k9.pkg	このファイルには、ホスト スキャン ソフトウェア、ホスト スキャン ライブラリ、サポート表など、Cisco Secure Desktop のすべての機能が含まれています。 この方式には、Cisco Secure Desktop 用の別個のライセンスが必要です。

ASA 上でのホスト スキャンのインストールと有効化

ホスト スキャンのインストールまたはアップグレード

次の手順を使用して、ASA 上で新しいホスト スキャン イメージをアップロードまたはアップグレードし、有効にすることができます。このイメージによって、AnyConnect のホスト スキャン機能をイネーブルにすることができます。また、このイメージを使用して、Cisco Secure Desktop（CSD）の既存の配置のホスト スキャン サポート表をアップグレードできます。

フィールドに、スタンドアロンのホスト スキャン パッケージ、または AnyConnect セキュア モビリティ クライアント パッケージのバージョン 3.0 以降を指定することができます。

以前に CSD イメージを ASA にアップロードしていた場合は、指定するホスト スキャン イメージによって、CSD パッケージに同梱されていた既存のホスト スキャン ファイルがアップグレードまたはダウングレードされます。

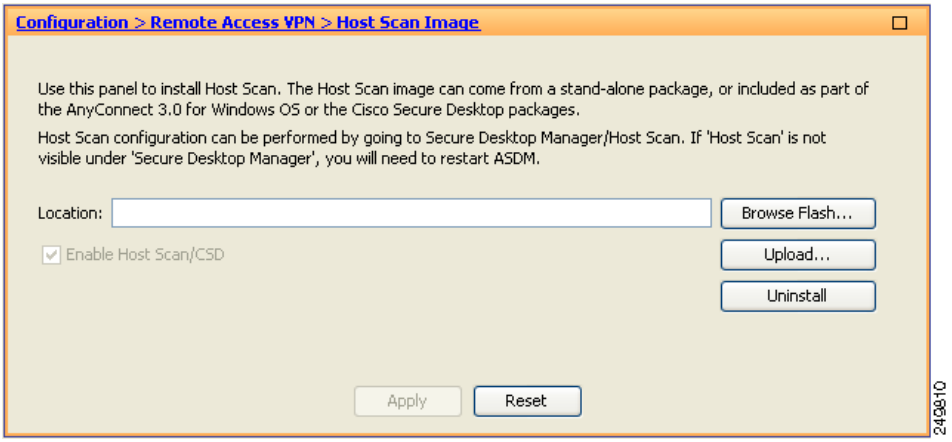
ホスト スキャンをインストールまたはアップグレードした後に、セキュリティ アプライアンスを再起動する必要はありませんが、Secure Desktop Manager にアクセスするには、Adaptive Security Device Manager（ASDM）を終了して再起動する必要があります。

（注） ホスト スキャンには、AnyConnect セキュア モビリティ クライアント Premium ライセンスが必要です。

ステップ 1　**hostscan**_*version*-**k9.pkg** ファイルまたは **anyconnect-NGC-win-*version*-k9.pkg** ファイルをコンピュータにダウンロードします。

ステップ 2　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。[Host Scan Image] パネルが開きます。

図 3-7　[Host Scan Image] パネル



ステップ 3　[Upload] をクリックして、ご使用のコンピュータから ASA 上のドライブにホスト スキャン パッケージのコピーを転送する準備をします。

ステップ 4　[Upload Image] ダイアログボックスで、[Browse Local Files] をクリックしてローカル コンピュータのホスト スキャン パッケージを検索します。

ステップ 5　ステップ 1 でダウンロードした **hostscan**_*version*.**pkg** ファイルまたは **anyconnect-NGC-win-*version*-k9.pkg** ファイルを選択し、[Select] をクリックします。[Local File Path] フィールドおよび [Flash File System Path] フィールドで選択したファイルのパスには、ホスト スキャン パッケージのアップロード先パスが反映されます。ASA に複数のフラッシュ ドライブがある場合は、別のフラッシュ ドライブを示すように [Flash File System Path] を編集できます。

ステップ 6　[Upload File] をクリックします。ASDM によって、ファイルのコピーがフラッシュ カードに転送されます。[Information] ダイアログボックスには、次のメッセージが表示されます。

```
File has been uploaded to flash successfully.
```

ステップ 7　[OK] をクリックします。

ステップ 8　[Use Uploaded Image] ダイアログで [OK] をクリックして、現行イメージとしてアップロードしたホスト スキャン パッケージ ファイルを使用します。

ステップ 9　[Enable Host Scan/CSD] がオンになっていない場合はオンにします。

ステップ 10　[Apply] をクリックします。

（注）　ASA 上で AnyConnect Essentials がイネーブルになっている場合、CSD は AnyConnect Essentials と組み合わせて動作しないというメッセージが表示されます。AnyConnect Essentials を**無効**にするか、**保持**するかを選択します。

ステップ 11　[File] メニューから [Save Running Configuration To Flash] を選択します。

ホスト スキャンの有効化または無効化

ASDM を使用して初めてホスト スキャン イメージをインストールまたはアップグレードする場合は、手順の一部としてそのイメージをイネーブルにします。「ASA 上でのホスト スキャンのインストールと有効化」（P.3-107）を参照してください。

それ以外の場合、ASDM を使用してホスト スキャン イメージを有効または無効にするには、次の手順を実行します。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。[Host Scan Image] パネル（図 3-7）が開きます。

ステップ 2　[Enable Host Scan/CSD] をオンにしてホスト スキャンを有効にするか、または [Enable Host Scan/CSD] をオフにしてホスト スキャンを無効にします。

ステップ 3　[Apply] をクリックします。

ASA 上での CSD の有効化または無効化

CSD をイネーブルにすると、CSD 設定ファイルである data.xml がフラッシュ デバイスから実行コンフィギュレーションにロードされます。

CSD を無効にしても、CSD 設定は変更されません。

次の手順に従い、ASDM を使用して CSD を有効または無効にします。

ステップ 1　[Configuration] > [Clientless SSL VPN] > [Secure Desktop] > [Setup] を選択します。

ASDM によって、[Setup] ペインが開きます（図 3-7）。

（注）　[Secure Desktop Image] フィールドに現在インストールされているイメージ（およびバージョン）が表示されます。[Enable Secure Desktop] チェックボックスは、CSD が有効になっているかどうかを示します。

ステップ 2　[Enable Secure Desktop] をオンかオフにして、[Apply] をクリックします。

ASDM によって、CSD がイネーブルまたはディセーブルになります。

ステップ 3　ASDM ウィンドウの右上にある [X] をクリックして終了します。

次のメッセージがウィンドウに表示されます。

```
The configuration has been modified.Do you want to save the running configuration to flash memory?
```

ステップ 4　[Save] をクリックします。ASDM は設定を保存して閉じます。

ASA でイネーブルになっているホスト スキャンのバージョンの表示

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] に移動します。

[Host Scan Image Location] フィールドにホスト スキャン イメージが指定されており、[Enable HostScan/CSD] ボックスがオンになっている場合は、そのイメージのバージョンが ASA で使用されるホスト スキャン バージョンとなります。

[Host Scan Image] フィールドが空で、[Enable HostScan/CSD] ボックスがオンになっている場合は、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] に移動します。[Secure Desktop Image Location] フィールドの CSD のバージョンが、ASA で使用されるホスト スキャン バージョンとなります。

ホスト スキャンのアンインストール

ホスト スキャン パッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、ホスト スキャンまたは CSD がイネーブルの場合でも ASA によるホスト スキャン パッケージの展開が回避されます。ホスト スキャンをアンインストールしても、フラッシュ ドライブのホスト スキャン パッケージは削除されません。

次の手順に従って、セキュリティ アプライアンス上のホスト スキャンをアンインストールします。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] に移動します。

ステップ 2　[Host Scan Image] ペインで [Uninstall] をクリックします。ASDM では、[Location] テキスト ボックスのテキストが削除されます。

ステップ 3　[File] メニューから [Save Running Configuration to Flash] を選択します。

ASA からの CSD のアンインストール

CSD をアンインストールすると、フラッシュ カード上のデスクトップ ディレクトリから CSD コンフィギュレーション ファイルである data.xml が削除されます。このファイルを保存する場合は、CSD をアンインストールする前に、別の名前を使用してファイルをコピーするか、ワークステーションにダウンロードします。

次の手順に従って、セキュリティ アプライアンス上の CSD をアンインストールします。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Setup] を選択します。

ASDM によって、[Setup] ペインが開きます（図 3-7）。

ステップ 2　[Uninstall] をクリックします。

次のメッセージが確認ウィンドウに表示されます。

```
Do you want to delete disk0:/csd_<n>.<n>.*.pkg and all CSD data files?
```

ステップ 3　[Yes] をクリックします。

ASDM によって、[Location] テキスト ボックスからテキストが削除され、[Setup] の下にある [Secure Desktop Manager] メニュー オプションが削除されます。

ステップ 4　ASDM ウィンドウの右上にある [X] をクリックして終了します。

次のメッセージがウィンドウに表示されます。

```
The configuration has been modified.Do you want to save the running configuration to flash memory?
```

ステップ 5　[Save] をクリックします。ASDM は設定を保存して閉じます。

AnyConnect ポスチャ モジュールのグループ ポリシーへの割り当て

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] の順に選択します。

ステップ 2　[Group Policies] パネルで [Add] をクリックして新規グループ ポリシーを作成するか、またはホスト スキャン パッケージを割り当てる既存のグループ 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] パネルで、左側の [Advanced] ナビゲーション ツリーを展開し、[AnyConnect Client] を選択します。

ステップ 4　[Optional Client Modules to Download Inherit] チェックボックスをオフにします。

ステップ 5　[Optional Client Modules to Download] ドロップダウン メニューで [AnyConnect Posture Module] をオンにし、[OK] をクリックします。

ステップ 6　[OK] をクリックします。

ホスト スキャンに関するその他の重要なマニュアル

ホスト スキャンがエンドポイント コンピュータからポスチャ クレデンシャルを収集した後は、情報を活用するために、ユーザはプリログイン ポリシーの設定、ダイナミック アクセス ポリシーの設定、Lua の式の使用などのサブジェクトを理解する必要があります。

これらの内容については、次のマニュアルで詳しく説明します。

- 『Cisco Secure Desktop Configuration Guides』
- 『Cisco Adaptive Security Device Manager Configuration Guides』

また、AnyConnect クライアントでのホスト スキャンの動作の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0*』を参照してください。

VPN セッションの最大数の設定

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

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

ステップ 2　[Maximum AnyConnect Sessions] フィールドに、許可されたセッションの最大数を入力します。

有効値は、1 からのライセンスで許容されるセッションの最大数までです。

ステップ 3　[Maximum Other VPN Sessions] フィールドに、許容された VPN セッションの最大数を入力します。これには、Cisco VPN クライアント（IPsec IKEv1）LAN-to-LAN VPN、およびクライアントレス SSL VPN セッションが含まれます。

有効値は、1 からのライセンスで許容されるセッションの最大数までです。

ステップ 4　[Apply] をクリックします。

暗号化コアのプールの設定

AnyConnect TLS/DTLS トラフィックに対してより適切なスループット パフォーマンスが得られるように、対称型マルチプロセッシング（SMP）プラットフォーム上での暗号化コアの割り当てを変更することができます。この変更によって、SSL VPN データパスが高速化され、AnyConnect、スマート トンネル、およびポート転送において、ユーザが認識できるパフォーマンス向上が実現します。暗号化コアのプールを設定するには、次の手順を実行します。

制限事項

- 暗号化コア再分散ができるのは、次のプラットフォームです。
  - 5585-X
  - 5545-X
  - 5555-X
  - ASASM

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

ステップ 2　[Accelerator Bias] ドロップダウン リストから、次のいずれかを選択します。

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

- [balanced]：暗号化ハードウェア リソースを均等に分散します（Admin/SSL および IPsec コア）。
- [ipsec]：IPsec を優先するように暗号化ハードウェア リソースを割り当てます（SRTP 暗号化音声トラフィックを含む）。
- [ssl]：Admin/SSL を優先するように暗号化ハードウェア リソースを割り当てます。

ステップ 3　[Apply] をクリックします。

	コマンド	目的
ステップ 1	`asa1(config)# crypto engine ?` `asa1(config)# crypto engine accelerator-bias ?`	暗号アクセラレータ プロセッサの割り当てを指定します。 • balanced：暗号ハードウェア リソースを均等に分散します。 • ipsec：暗号ハードウェア リソースを優先 IPsec/暗号化音声（SRTP）に割り当てます。 • ssl：暗号ハードウェア リソースを優先 SSL に割り当てます。

ISE ポリシー実施の設定

Cisco Identity Services Engine（ISE）は、セキュリティ ポリシー管理および制御プラットフォームです。有線、ワイヤレス、VPN 接続のアクセス制御とセキュリティ コンプライアンスを自動化し、シンプルにします。Cisco ISE は主に、Cisco TrustSec と連携してセキュアなアクセスおよびゲスト アクセスを提供し、BYOD に対する取り組みをサポートし、使用ポリシーを適用するために使用されます。

ISE Change of Authorization（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザ グループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インライン ポスチャ実施ポイント（IPEP）で、ASA と確立された各 VPN セッションのアクセス コントロール リスト（ACL）を適用する必要がなくなりました。

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

- IPSec
- AnyConnect
- L2TP/IPSec

システム フローは次のとおりです。

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

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

認可変更のための AAA サーバ グループの設定

次の手順は、認可変更の設定例を示しています。

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] を選択します。

ステップ 2　RADIUS プロトコルを使用する AAA サーバ グループを作成するか、既存の AAA サーバ グループを編集します。

ステップ 3　[Accounting Mode] として [Single] を選択します。

ステップ 4　[Reactivation Mode] として [Depletion] を選択します。

ステップ 5　[Dead Time] フィールドに **10** と入力します。

ステップ 6　[Max Failed Attempts] フィールドに **3** と入力します。

ステップ 7　[Enable Interim Accounting Update] チェックボックスをオンにします。

ステップ 8　[Update Interval] フィールドに **1** と入力します。

ステップ 9　[Enable Active Directory Agent Mode] チェックボックスがオフになっていることを確認します。

ステップ 10　[Enable Dynamic Authorization] チェックボックスをオンにします。

ステップ 11　[Dynamic Authorization Port] フィールドに **1700** と入力します。

ステップ 12　[Use Authorization Only Mode] チェックボックスをオンにします。

ステップ 13　[OK] をクリックして変更を適用します。または、[Cancel] をクリックして変更を破棄します。

詳細については、一般的な操作のコンフィギュレーション ガイドの「AAA の RADIUS サーバの設定」の章を参照してください。

AnyConnect における AAA サーバの任意のステップの設定

AnyConnect を使用している場合は、トンネル グループの [AnyConnect Connection Profile] 画面でそのトンネル グループの URL を指定することも必要になります。

ステップ 1　必要なトンネル グループの [AnyConnect Connection Profile] 画面に移動します。

ステップ 2　[Group URLs] セクションで [Add] をクリックし、http://10.10.10.4/ISE-Tunnel-Group などの URL を入力します。

ステップ 3　[Enabled] チェックボックスがオンになっていることを確認します。

ステップ 4　[OK] をクリックして変更を適用します。

（注）　この機能のトラブルシューティングについては、VPN コンフィギュレーション ガイドの「ISE ポリシー実施の設定」の項を参照してください。

VPN の IP アドレス

この章では、IP アドレスの割り当て方式について説明します。

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。

IP アドレスの割り当てポリシーの設定

ASA では、リモート アクセス クライアントに IP アドレスを割り当てる際に、次の 1 つ以上の方式を使用することができます。複数のアドレス割り当て方式を設定すると、ASA は IP アドレスが見つかるまで各オプションを検索します。デフォルトでは、すべての方式がイネーブルになっています。

- [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。

次の方法のいずれかを使用して、IP アドレスをリモート アクセス クライアントに割り当てる方法を指定します。

- 「ASDM を使用した IP アドレス割り当てオプションの設定」

ASDM を使用した IP アドレス割り当てオプションの設定

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。IPv4 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。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

アドレス割り当て方式の表示

ASA で設定されているアドレス割り当て方式を表示するには、次のいずれかの方式を使用します。

ASDM を使用した IPv4 および IPv6 のアドレス割り当ての表示

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

ローカル IP アドレス プールの設定

VPN リモート アクセス トンネルに対して 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。

ローカル IP アドレス プールを設定するには、次のいずれかの方法を使用します。

- 「ASDM を使用したローカル IPv4 アドレス プールの設定」（P.4-3）
- 「ASDM を使用したローカル IPv6 アドレス プールの設定」（P.4-4）

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　[Apply] をクリックします。

ステップ 5　[OK] 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　[Apply] をクリックします。

ステップ 5　[OK] をクリックします。

DHCP アドレッシングの設定

DHCP を使用して VPN クライアントのアドレスを割り当てるには、まず DHCP サーバ、およびその DHCP サーバで使用可能な IP アドレスの範囲を設定する必要があります。その後、接続プロファイル単位で DHCP サーバを定義します。また、オプションとして、該当の接続プロファイルまたはユーザ名に関連付けられたグループ ポリシー内に、DHCP ネットワーク スコープも定義できます。このスコープは、使用する IP アドレス プールを DHCP サーバに指定するための、IP ネットワーク番号または IP アドレスです。

次の例では、**firstgroup** という名前の接続プロファイルに、IP アドレス 172.33.44.19 の DHCP サーバを定義しています。また、この例では、**remotegroup** というグループ ポリシーに対して、192.86.0.0 という DHCP ネットワーク スコープも定義しています（remotegroup というグループ ポリシーは、firstgroup という接続プロファイルに関連付けられています）。ネットワーク スコープを定義しない場合、DHCP サーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

次のコンフィギュレーションには、本来不要な手順が含まれています。これらは、以前にその接続プロファイルに名前を付け、接続プロファイル タイプをリモート アクセスとして定義していたり、グループ ポリシーに名前を付け、内部または外部として指定していた場合のためです。これらの手順が次の例に記載されているのは、これらの値を設定しない限り、後続の tunnel-group コマンドおよび group-policy コマンドにアクセスできないので、注意を促すためです。

注意事項と制約事項

IPv4 アドレスを使用して、クライアント アドレスを割り当てる DHCP サーバを識別できます。

DHCP を使用した IP アドレスの割り当て

DHCP サーバを設定してから、DHCP サーバを使用するグループ ポリシーを作成します。そのグループ ポリシーを選択すると、DHCP サーバが VPN 接続のアドレスを割り当てます。

DHCP サーバの設定

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] で DHCP がイネーブルになっていることを確認します。

ステップ 3　[Configuration] > [Remote Access VPN] > [DHCP Server] を選択して、DHCP サーバを設定します。

グループ ポリシーへの DHCP IP アドレスの割り当て

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。

ステップ 2　[Connection Profiles] エリアで [Add] または [Edit] をクリックします。

ステップ 3　接続プロファイルの設定ツリーで、[Basic] をクリックします。

ステップ 4　[Client Address Assignment] エリアで、クライアントに IP アドレスを割り当てるために使用する DHCP サーバの IPv4 アドレスを入力します。たとえば、**172.33.44.19** と指定します。

ステップ 5　DHCP スコープを定義するために、接続プロファイルに関連付けられたグループ ポリシーを編集します。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 6　編集するグループ ポリシーをダブルクリックします。

ステップ 7　設定ツリーで、[Servers] をクリックします。

ステップ 8　下矢印をクリックして、[More Options] エリアを拡大表示します。

ステップ 9　DHCP スコープの [Inherit] のチェックを外します。

ステップ 10　使用する IP アドレス プールを DHCP サーバに指定するための、IP ネットワーク番号または IP アドレスを入力します。たとえば、**192.86.0.0** と指定します。

ステップ 11　[OK] をクリックします。

ステップ 12　[Apply] をクリックします。

ローカル ユーザへの IP アドレスの割り当て

グループ ポリシーを使用するようにローカル ユーザ アカウントを設定し、また AnyConnect 属性を設定することもできます。IP アドレスの他のソースに障害が発生した場合に、これらのユーザ アカウントがフォールバックを提供するので、管理者は引き続きアクセスできます。

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、一般的な操作のコンフィギュレーション ガイドを参照してください。

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。

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。

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 ポリシーの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。
- [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）接続では IPsec IKEv1 が使用されます。
- [IPsec IKEv2] : AnyConnect セキュア モビリティ クライアント対応の 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、ログオン 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オン数を指定します。Simultaneous Logons パラメータは、このユーザに指定できる最大同時ログオン数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログオンが無効になり、ユーザ アクセスを禁止します。

（注）　最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

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（オプション）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（オプション）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。

CHAPTER 5

ダイナミック アクセス ポリシー

この章では、ダイナミック アクセス ポリシーを設定する方法を説明します。次の項目を取り上げます。

ダイナミック アクセス ポリシーについて

VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザが持つさまざまなロール、および設定とセキュリティ レベルが異なるリモート アクセス サイトからのログインなど、複数の変数が影響する可能性があります。VPN 環境でのユーザ認可のタスクは、スタティックな設定のネットワークでの認可タスクよりもかなり複雑です。

ASA でのダイナミック アクセス ポリシー（DAP）により、これらの多くの変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザ トンネルまたはユーザ セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。つまり、ASA では、定義したポリシーに基づき、特定のユーザに対して、特定のセッションのアクセスが許可されます。ASA は、ユーザが接続した時点で、1 つ以上の DAP レコードから属性を選択または集約することによって DAP を生成します。DAP レコードは、リモート デバイスのエンドポイント セキュリティ情報および認証されたユーザの AAA 認可情報に基づいて選択されます。選択された DAP レコードは、ユーザ トンネルまたはセッションに適用されます。

DAP システムには、注意を必要とする次のコンポーネントがあります。

- DAP 選択コンフィギュレーション ファイル：セッション確立中に DAP レコードを選択および適用するために ASA が使用する、基準が記述されたテキスト ファイル。ASA に保存されています。ASDM を使用して、このファイルを変更したり、XML データ形式で ASA にアップロードしたりできます。DAP 選択コンフィギュレーション ファイルには、ユーザが設定するすべての属性が記載されています。これには、AAA 属性、エンドポイント属性、およびネットワーク ACL と Web タイプ ACL のフィルタで設定されるアクセス ポリシー、ポート転送、URL のリストなどがあります。
- DfltAccess ポリシー：常に DAP サマリー テーブルの最後のエントリで、プライオリティは必ず 0。デフォルト アクセス ポリシーのアクセス ポリシー属性を設定できますが、AAA 属性またはエンドポイント属性は含まれておらず、これらの属性は設定できません。DfltAccessPolicy は削除できません。また、サマリー テーブルの最後のエントリになっている必要があります。

詳細については、『*Dynamic Access Deployment Guide*』（https://supportforums.cisco.com/docs/DOC-1369）を参照してください。

DAP によるリモート アクセス プロトコルおよびポスチャ評価ツールのサポート

ASA は、管理者が設定したポスチャ評価ツールを使用してエンドポイント セキュリティ属性を取得します。このポスチャ評価ツールには、AnyConnect ポスチャ モジュール、独立したホスト スキャン パッケージ、Cisco Secure Desktop、NAC などがあります。

次の表に、DAP がサポートしている各リモート アクセス プロトコル、その方式で使用可能なポスチャ評価ツール、およびそのツールによって提供される情報を示します。

サポートされるリモート アクセス プロトコル	**AnyConnect ポスチャ モジュール ホスト スキャン パッケージ Cisco Secure Desktop （Endpoint Assessment ホスト スキャン拡張機能がイネーブルでない）**	**AnyConnect ポスチャ モジュール ホスト スキャン パッケージ Cisco Secure Desktop （Endpoint Assessment ホスト スキャン拡張機能がイネーブルである）**	**NAC**	**Cisco NAC アプライアンス**
	ファイル情報、レジストリ キーの値、実行プロセス、オペレーティング システムを返す	アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール ソフトウェアの情報を返す	NAC ステータスを返す	VLAN タイプと VLAN ID を返す
IPsec VPN	No	No	Yes	Yes
Cisco AnyConnect VPN	Yes	Yes	Yes	Yes
クライアントレス（ブラウザベース）SSL VPN	Yes	Yes	No	No
PIX カットスルー プロキシ（ポスチャ評価は使用不可）	No	No	No	No

DAP を使用するリモート アクセス接続シーケンス

次のシーケンスは、標準的なリモート アクセス接続を確立する場合の概要を示しています。

1. リモート クライアントが VPN 接続を試みます。
2. ASA は、設定された NAC 値と Cisco Secure Desktop の Host Scan 値を使用してポスチャ評価を実行します。
3. ASA が、AAA を介してユーザを認証します。AAA サーバは、ユーザの認可属性も返します。
4. ASA が、AAA 認可属性をそのセッションに適用し、VPN トンネルを確立します。
5. ASA が、AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。
6. ASA が、選択した DAP レコードから DAP 属性を集約します。集約された属性が DAP ポリシーを構成します。
7. ASA がその DAP ポリシーをセッションに適用します。

ダイナミック アクセス ポリシーのライセンス

（注）　この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件
ASAv	Premium ライセンス
他のすべてのモデル	AnyConnect Premium ライセンス Advanced Endpoint Assessment ライセンス AnyConnect Mobile ライセンス

（注）　ASA 管理者が AnyConnect モバイル ポスチャ DAP 属性をどのように使用するかは、インストール済みの AnyConnect ライセンスによって異なります。詳細については、「DAP への AnyConnect エンドポイント属性の追加」（P.5-11）を参照してください。

ダイナミック アクセス ポリシーの設定

はじめる前に

- 特に記載のない限り、DAP エンドポイント属性を設定する前に Cisco Secure Desktop またはホスト スキャンをインストールする必要があります。
- ファイル、プロセス、レジストリのエンドポイント属性を設定する前に、ファイル、プロセス、レジストリの基本ホスト スキャン属性を設定する必要があります。手順については、ASDM を起動して [Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] の順に選択し、[Help] をクリックしてください。
- DAP は、ASCII 文字のみサポートされます。

ステップ 1　ASDM を起動し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] または [Clientless SSL VPN Access] > [Dynamic Access Policies] の順に選択します。

ステップ 2　特定のアンチウイルス、アンチスパイウェア、またはパーソナル ファイアウォールのエンドポイント属性を含めるには、ペインの最上部近くの [CSD configuration] リンクをクリックします。次に、Cisco Secure Desktop およびホスト スキャンの拡張機能をイネーブルにします。このリンクは、これら両方の機能をすでにイネーブルにしている場合には表示されません。

Cisco Secure Desktop 拡張機能をイネーブルにしてホスト スキャン拡張機能はイネーブルにしない場合、変更を適用すると、ASDM は**ホスト スキャン コンフィギュレーション**をイネーブルにするリンクを表示します。

ステップ 3　設定済みの DAP のリストを表示します。テーブルには次のフィールドが表示されます。

- [ACL Priority]：DAP レコードのプライオリティを表示します。

  ASA は、複数の DAP レコードからネットワーク ACL と Web タイプ ACL を集約するときに、この値を使用して ACL を論理的に順序付けします。ASA は、最上位のプライオリティ番号から最下位のプライオリティ番号の順にレコードを並べ、最下位のプライオリティをテーブルの一番下に配置します。番号が大きいほどプライオリティが高いことを意味します。たとえば、値が 4 の DAP レコードは値が 2 のレコードよりも高いプライオリティを持つことになります。プライオリティは、手動での並べ替えはできません。
- [Name]：DAP レコードの名前を表示します。
- [Network ACL List]：セッションに適用されるファイアウォール ACL の名前を表示します。
- [Web-Type ACL List]：セッションに適用される SSL VPN ACL の名前を表示します。
- [Description]：DAP レコードの目的を説明します。

ステップ 4　[Add] または [Edit] をクリックして、「ダイナミック アクセス ポリシーの追加または編集」（P.5-4）を実行します。

ステップ 5　[Apply] をクリックして DAP 設定を保存します。

ステップ 6　[Find] フィールドを使用して、ダイナミック アクセス ポリシー（DAP）を検索します。

このフィールドへの入力を開始すると、DAP テーブルの各フィールドの先頭部分の文字が検索され、一致するものが検出されます。ワイルドカードを使用すると、検索範囲が広がります。

たとえば、[Find] フィールドに `sal` と入力すると、`Sales` という名前の DAP が一致しますが、`Wholesalers` という名前の DAP は一致しません。[Find] フィールドに `*sal` と入力した場合は、テーブル内の Sales と Wholesalers のうち、最初に出現するものが検出されます。

ステップ 7　「ダイナミック アクセス ポリシーのテスト」（P.5-5）を実行して設定を確認します。

ダイナミック アクセス ポリシーの追加または編集

ステップ 1　ASDM を起動し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] または [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add] または [Edit] の順に選択します。

ステップ 2　このダイナミック アクセス ポリシーの名前（必須）と説明（オプション）を入力します。

- [Policy Name] は、4 ～ 32 文字の文字列で、スペースは使用できません。
- DAP の [Description] フィールドには 80 文字まで入力できます。

ステップ 3　[ACL Priority] フィールドで、そのダイナミック アクセス ポリシーのプライオリティを設定します。

セキュリティ アプライアンスは、ここで設定した順序でアクセス ポリシーを適用します。数が大きいほどプライオリティは高くなります。有効値の範囲は 0 ～ 2147483647 です。デフォルト値は 0 です。

ステップ 4　この DAP の選択基準を指定します。

a. [Selection Criteria] ペインのドロップダウン リスト（ラベルなし）で、ユーザがこのダイナミック アクセス ポリシーを使用するには、すべてのエンドポイント属性を満たすことに加えて、ここで設定される AAA 属性値のいずれか（[ANY]）またはすべて（[ALL]）が必要となるのか、それとも一切不要（[NONE]）であるのかを選択します。

重複するエントリは許可されません。AAA またはエンドポイント属性なしの DAP レコードを設定すると、ASA は常にそのレコードを選択します。これは、そのレコードがすべての選択基準を満たすことになるからです。

b. [AAA Attributes] フィールドの [Add] または [Edit] をクリックして、「DAP の AAA 属性選択基準の設定」（P.5-6）を実行します。

c. [Endpoint Attributes] 領域の [Add] または [Edit] をクリックして、「DAP のエンドポイント属性選択基準の設定」（P.5-9）を実行します。

d. [Advanced] フィールドをクリックして、「Lua を使用した DAP における追加の DAP 選択基準の作成」（P.5-19）を実行します。この機能を使用するには、Lua プログラミング言語の知識が必要です。

- [AND/OR]：基本的な選択ルールと、ここで入力する論理式との関係を定義します。つまり、すでに設定されている AAA 属性およびエンドポイント属性に新しい属性を追加するのか、またはそれら設定済みの属性に置き換えるのかを指定します。デフォルト値は AND です。
- [Logical Expressions]：それぞれのタイプのエンドポイント属性のインスタンスを複数設定できます。新しい AAA またはエンドポイント選択属性を定義する自由形式の Lua を入力します。ASDM は、ここで入力されるテキストの検証を行わず、単にこのテキストを DAP XML ファイルにコピーします。ASA がそれを処理し、解析不能な式があれば破棄します。

ステップ 5　この DAP のアクセス/許可ポリシー属性を指定します。

ここで設定する属性値は、既存のユーザ、グループ、トンネル グループ、およびデフォルトのグループ レコードを含め、AAA システムの認可値を上書きします。「DAP アクセスと許可ポリシー属性の設定」（P.5-25）を参照してください。

ステップ 6　[OK] をクリックします。

ダイナミック アクセス ポリシーのテスト

このペインでは、認可属性値のペアを指定することによって、デバイスで設定される DAP レコード セットが取得されるかどうかをテストできます。

ステップ 1　属性値のペアを指定するには、[AAA Attribute] テーブルと [Endpoint Attribute] テーブルに関連付けられた [Add/Edit] ボタンを使用します。

[Add/Edit] ボタンをクリックすると表示されるダイアログは、[Add/Edit AAA Attributes] ウィンドウと [Add/Edit Endpoint Attributes] ダイアログボックスに表示されるダイアログに似ています。

ステップ 2　[Test] ボタンをクリックします。

デバイス上の DAP サブシステムは、各レコードの AAA およびエンドポイント選択属性を評価するときに、これらの値を参照します。結果は、[Test Results] 領域に表示されます。

DAP の AAA 属性選択基準の設定

DAP は AAA サービスを補完します。用意されている認可属性のセットは限られていますが、それらの属性によって AAA で提供される認可属性を無効にできます。AAA 属性は、Cisco AAA 属性階層から、または ASA が RADIUS または LDAP サーバから受信する一式の応答属性セットから指定できます。ASA は、ユーザの AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。ASA は、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 認可属性を作成します。

ステップ 1　DAP レコードの選択基準として AAA 属性を設定するには、[Add/Edit AAA Attributes] ダイアログボックスで、使用する Cisco、LDAP、または RADIUS 属性を設定します。これらの属性は、入力する値に対して「=」または「!=」のいずれかに設定できます。各 DAP レコードに設定可能な AAA 属性の数に制限はありません。AAA 属性の詳細については、「AAA 属性の定義」を参照してください。

[AAA Attributes Type]：ドロップダウン リストを使用して、Cisco、LDAP、または RADIUS 属性を選択します。

- [Cisco] : AAA 階層モデルに保存されているユーザ認可属性を参照します。DAP レコードの AAA 選択属性に、これらのユーザ認可属性の小規模なサブセットを指定できます。次の属性が含まれます。
  - [Group Policy] : VPN ユーザ セッションに関連付けられているグループ ポリシー名を示します。セキュリティ アプライアンスでローカルに設定するか、IETF-Class (25) 属性として RADIUS/LDAP から送信します。最大 64 文字です。
  - [Assigned IP Address] : ポリシーに指定する IPv4 アドレスを入力します。フル トンネル VPN クライアント（IPsec、L2TP/IPsec、SSL VPN AnyConnect）に割り当てられた IP アドレスは、クライアントレス SSL VPN には割り当てられません。クライアントレス セッションにはアドレスの割り当てがないからです。
  - [Assigned IPv6 Address]：ポリシーに指定する IPv6 アドレスを入力します。
  - [Connection Profile]：コネクションまたはトネリングのグループ名。最大 64 文字です。
  - [Username]：認証されたユーザのユーザ名。最大 64 文字です。ローカル認証、RADIUS 認証、LDAP 認証のいずれかを、またはその他の認証タイプ（RSA/SDI、NT Domain などのいずれかを使用している場合に適用されます。
  - [=/!=]：と等しい/と等しくない
- [LDAP]：LDAP クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ LDAP 応答属性値のペアを保存します。LDAP クライアントでは、受信した順に応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザ レコードとグループ レコードの両方が LDAP サーバから読み込まれると、このシナリオが発生する場合があります。ユーザ レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  Active Directory グループ メンバーシップをサポートするために、AAA LDAP クライアントでは、LDAP memberOf 応答属性に対する特別な処理が行われます。AD memberOf 属性は、AD 内のグループ レコードの DN 文字列を指定します。グループの名前は、DN 文字列内の最初の CN 値です。LDAP クライアントでは、DN 文字列からグループ名を抽出して、AAA memberOf 属性として格納し、応答属性データベースに LDAP memberOf 属性として格納します。LDAP 応答メッセージ内に追加の memberOf 属性が存在する場合、それらの属性からグループ名が抽出され、前の AAA memberOf 属性と結合されて、グループ名がカンマで区切られた文字列が生成されます。この文字列は応答属性データベース内で更新されます。

LDAP 認証/認可サーバへの VPN リモート アクセス セッションが次の 3 つの Active Directory グループ（memberOf 列挙）のいずれかを返す場合は、次のとおりとなります。

cn=Engineering,ou=People,dc=company,dc=com

cn=Employees,ou=People,dc=company,dc=com

cn=EastCoastast,ou=People,dc=company,dc=com

ASA は、Engineering、Employees、EastCoast の 3 つの Active Directory グループを処理します。これらのグループは、aaa.ldap の選択基準としてどのような組み合わせでも使用できます。

LDAP 属性は、DAP レコード内の属性名と属性値のペアで構成されています。LDAP 属性名は、構文に従う必要があり、大文字、小文字を区別します。たとえば、AD サーバが部門として返す値の代わりに、LDAP 属性の Department を指定した場合、DAP レコードはこの属性設定に基づき一致しません。

（注） [Value] フィールドに複数の値を入力するには、セミコロン（;）をデリミタとして使用します。次に例を示します。

eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- [RADIUS]：RADIUS クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ RADIUS 応答属性値のペアを保存します。RADIUS クライアントは、受け取った順序で応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザ レコードおよびグループ レコードの両方が RADIUS サーバから読み込まれた場合、このシナリオが発生する可能性があります。ユーザ レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  RADIUS 属性は、DAP レコード内の属性番号と属性値のペアで構成されています。セキュリティ アプライアンスがサポートする RADIUS 属性の一覧を示す表については、「セキュリティ アプライアンスがサポートする RADIUS の属性と値」を参照してください。

  （注） RADIUS 属性について、DAP は Attribute ID = 4096 + RADIUS ID と定義します。

  次に例を示します。

  RADIUS 属性「Access Hours」の Radius ID は 1 であり、したがって DAP 属性値は 4096 + 1 = 4097 となります。

  RADIUS 属性「Member Of」の Radius ID は 146 であり、したがって DAP 属性値は 4096 + 146 = 4242 となります。

- LDAP および RADIUS 属性には、次の値があります。
  - [Attribute ID]：属性の名前/番号。最大 64 文字です。
  - [Value]：属性名（LDAP）または数値（RADIUS）。

    [Value] フィールドに複数の値を入力するには、セミコロン（;）をデリミタとして使用します。次に例を示します。

    ```
    eng;sale; cn=Audgen VPN,ou=USERS,o=OAG
    ```
  - [=/!=]：と等しい/と等しくない
- LDAP には、[Get AD Groups] ボタンが含まれます。「Active Directory グループの取得」（P.5-8）を参照してください。

Active Directory グループの取得

Active Directory サーバにクエリーを実行し、このペインで利用可能な AD グループを問い合わせることができます。この機能は、LDAP を使用している Active Directory サーバだけに適用されます。このボタンは、Active Directory LDAP サーバに対して、ユーザが属するグループのリスト（memberOf 列挙）の問い合わせを実行します。このグループ情報を使用し、ダイナミック アクセス ポリシーの AAA 選択基準を指定します。

AD グループは、CLI の **show-ad-groups** コマンドをバックグランドで実行することで LDAP サーバから取得されます。ASA がサーバの応答を待つデフォルト時間は 10 秒です。この時間は、AAA サーバ ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用して調整できます。

[Edit AAA Server] ペインで Group Base DN を変更し、Active Directory 階層の中で検索を開始するレベルを変更できます。ウィンドウ内で、ASA がサーバの応答を待つ時間も変更できます。これらの機能を設定するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] > [Edit AAA Server] の順に選択します。

（注） Active Directory サーバにあるグループが多数である場合、取得した AD グループのリスト（**show ad-groups** コマンドの出力）はサーバが応答パケットに含めることのできるデータ量の制限に従い切り捨てられることがあります。この問題を回避するには、フィルタ機能を使用して、サーバから返されるグループの数を減らしてください。

[AD Server Group]：AD グループを取得する AAA サーバ グループ名。

[Filter By]：表示されるグループを減らすために、グループ名またはグループ名の一部を指定します。

[Group Name]：サーバから取得された AD グループのリスト。

AAA 属性の定義

次の表に、DAP で使用できる AAA 選択属性名の定義を示します。属性名フィールドは、Lua 論理式での各属性名の入力方法を示しており、[Add/Edit Dynamic Access Policy] ペインの [Advanced] セクションで使用します。

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
Cisco	aaa.cisco.grouppolicy	AAA	ストリング	64	ASA 上にある、または RADIUS/LDAP サーバから IETF-CLass (25) 属性として送信されたグループ ポリシー名
	aaa.cisco.ipaddress	AAA	数値	-	フル トンネル VPN クライアントに割り当てられた IP アドレス（IPsec、L2TP/IPsec、SSL VPN AnyConnect）
	aaa.cisco.tunnelgroup	AAA	ストリング	64	接続プロファイル（トンネル グループ）の名前
	aaa.cisco.username	AAA	ストリング	64	認証されたユーザの名前（ローカル認証や認可を使用している場合に適用）

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
LDAP	aaa.ldap.<*label*>	LDAP	ストリング	128	LDAP 属性値ペア
RADIUS	aaa.radius.<number>	RADIUS	ストリング	128	RADIUS 属性値ペア

セキュリティ アプライアンスがサポートする RADIUS 属性の一覧を示す表については、「セキュリティ アプライアンスがサポートする RADIUS の属性と値」を参照してください。

DAP のエンドポイント属性選択基準の設定

エンドポイント属性には、エンドポイント システム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。ASA は、エンドポイント属性の集合をセッション確立時に動的に生成し、セッションに関連付けられたデータベースにその属性を保存します。各 DAP レコードには、ASA がセッションの DAP レコードを選択するために満たす必要があるエンドポイント選択属性が指定されます。ASA は、設定されたすべての条件を満たす DAP レコードだけを選択します。

はじめる前に

- DAP レコードの選択基準としてエンドポイント属性を設定することは、「ダイナミック アクセス ポリシーの設定」（P.5-3）という大きなプロセスの一部です。DAP の選択基準としてエンドポイント属性を設定する前に、この手順を確認してください。
- エンドポイント属性の詳細については、「エンドポイント属性の定義」を参照してください。
- ホスト スキャンがアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォールの各メモリ常駐型プログラムをチェックする方法の詳細については、「DAP とアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラム」（P.5-16）を参照してください。

ステップ 1　[Add] または [Edit] をクリックして、次のいずれかのエンドポイント属性を選択基準として追加します。

各タイプのエンドポイント属性のインスタンスを複数作成できます。各 DAP レコードに設定可能なエンドポイント属性の数に制限はありません。

- 「DAP へのアンチスパイウェア/アンチウイルス エンドポイント属性の追加」（P.5-10）
- 「DAP へのアプリケーション属性の追加」（P.5-10）
- 「DAP への AnyConnect エンドポイント属性の追加」（P.5-11）
- 「DAP へのファイル エンドポイント属性の追加」（P.5-12）
- 「DAP へのデバイス エンドポイント属性の追加」（P.5-13）
- 「DAP への NAC エンドポイント属性の追加」（P.5-13）
- 「DAP へのオペレーティング システム エンドポイント属性の追加」（P.5-14）
- 「DAP へのパーソナル ファイアウォール エンドポイント属性の追加」（P.5-14）
- 「DAP へのポリシー エンドポイント属性の追加」（P.5-14）
- 「DAP へのプロセス エンドポイント属性の追加」（P.5-15）
- 「DAP へのレジストリ エンドポイント属性の追加」（P.5-15）

ステップ 2　条件に一致する DAP ポリシーを指定します。

これらのエンドポイント属性のタイプごとに、ユーザがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND、デフォルト）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを決定します。

a. [Logical Op] をクリックします。

b. エンドポイント属性のタイプごとに、[Match Any]（デフォルト）または [Match All] を選択します。

c. [OK] をクリックします。

ステップ 3　「ダイナミック アクセス ポリシーの追加または編集」（P.5-4）に戻ってください。

DAP へのアンチスパイウェア/アンチウイルス エンドポイント属性の追加

ステップ 1　[Endpoint Attribute Type] リスト ボックスで、[Anti-Spyware] または [Anti-Virus] を選択します。

ステップ 2　適切なボタン [Enabled]、[Disabled]、または [Not Installed] をクリックして、選択したエンドポイント属性とそれに付随する修飾子（[Enabled]/[Disabled]/[Not Installed] ボタンの下のフィールド）をイネーブルにするか、ディセーブルにするか、またはインストールしないかを指定します。

ステップ 3　[Vendor ID] リスト ボックスで、テスト対象のアンチスパイウェアまたはアンチウイルスのベンダーの名前をクリックします。

ステップ 4　[Product Description] チェックボックスをオンにして、テストするベンダーの製品名をリスト ボックスから選択します。

ステップ 5　[Version] チェックボックスをオンにして、操作フィールドを、[Version] リスト ボックスで選択した製品バージョン番号に等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）に設定します。

[Version] リスト ボックスで選択したバージョンに x が付いている場合（たとえば 3.x）は、この x を具体的なリリース番号で置き換えます（たとえば 3.5）。

ステップ 6　[Last Update] チェックボックスをオンにします。最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。

ステップ 7　[OK] をクリックします。

DAP へのアプリケーション属性の追加

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [Application] を選択します。

ステップ 2　[Client Type] の操作フィールドで、[=]（等しい）または [!=]（等しくない）を選択します。

ステップ 3　[Client type] リスト ボックスで、テスト対象のリモート アクセス接続のタイプを指定します。

ステップ 4　[OK] をクリックします。

DAP への AnyConnect エンドポイント属性の追加

AnyConnect エンドポイント属性（モバイル ポスチャまたは AnyConnect アイデンティティ拡張機能（ACIDex）とも呼ばれる）は、AnyConnect VPN クライアントが ASA にポスチャ情報を伝えるために使用されます。ダイナミック アクセス ポリシーでは、このエンドポイント属性を使用してユーザを認可します。

モバイル ポスチャ属性をダイナミック アクセス ポリシーに組み込むと、エンドポイントにホスト スキャンや Cisco Secure Desktop がエンドポイントにインストールされていなくても適用できます。

モバイル ポスチャ属性の一部は、モバイル デバイスのみを実行している AnyConnect クライアントに関連し、一部のモバイル ポスチャ属性は、モバイル デバイスを実行している AnyConnect クライアントおよび AnyConnect デスクトップ クライアントの両方に関連しています。

はじめる前に

モバイル ポスチャを活用するには、AnyConnect Mobile ライセンスと、AnyConnect Essentials ライセンスが ASA にインストールされている必要があります。これらのライセンスをインストールする企業は、DAP 属性および他の既存のエンドポイント属性に基づいてサポートされているモバイル デバイスの DAP ポリシーを適用できます。これには、モバイル デバイスからのリモート アクセスの許可または拒否が含まれます。

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [AnyConnect] を選択します。

ステップ 2　[Client Version] チェックボックスをオンにして、等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）を操作フィールドで選択してから、[Client Version] フィールドで AnyConnect クライアント バージョン番号を指定します。

このフィールドを使用すると、モバイル デバイス（携帯電話やタブレットなど）のクライアント バージョンを評価できるほか、デスクトップやラップトップ デバイスのクライアント バージョンも評価できます。

ステップ 3　[Platform] チェックボックスをオンにして、等しい（=）または等しくない（!=）を操作フィールドで選択してから、[Platform] リスト ボックスでオペレーティング システムを選択します。

このフィールドを使用すると、モバイル デバイス（携帯電話やタブレットなど）のオペレーティング システムを評価できるほか、デスクトップやラップトップ デバイスのオペレーティング システムも評価できます。プラットフォームを選択すると、追加の属性フィールドである [Device Type] と [Device Unique ID] が使用可能になります。

ステップ 4　[Platform Version] チェックボックスをオンにして、等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）を操作フィールドで選択してから、[Platform Version] フィールドでオペレーティング システム バージョン番号を指定します。

作成する DAP レコードにこの属性も含まれるようにするには、前の手順でプラットフォームも必ず指定してください。

ステップ 5　[Platform] チェックボックスをオンにした場合は、[Device Type] チェックボックスをオンにすることができます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、デバイスを [Device Type] フィールドで選択するか入力します。

サポートされるデバイスであるにもかかわらず、[Device Type] フィールドのリストに表示されていない場合は、[Device Type] フィールドに入力できます。デバイス タイプ情報を入手する最も確実な方法は、AnyConnect クライアントをエンドポイントにインストールして ASA に接続し、DAP トレースを実行することです。DAP トレースの結果の中で、**endpoint.anyconnect.devicetype** の値を見つけます。この値を [Device Type] フィールドに入力する必要があります。

ステップ 6　[Platform] チェックボックスをオンにした場合は、[Device Unique ID] チェックボックスをオンにすることができます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、デバイスの一意の ID を [Device Unique ID] フィールドに入力します。

[Device Unique ID] によって個々のデバイスが区別されるので、特定のモバイル デバイスに対するポリシーを設定できます。デバイスの一意の ID を取得するには、そのデバイスを ASA に接続して DAP トレースを実行し、**endpoint.anyconnect.deviceuniqueid** の値を見つける必要があります。この値を [Device Unique ID] フィールドに入力する必要があります。

ステップ 7　[Platform] をオンにした場合は、[MAC Addresses Pool] フィールドに MAC アドレスを追加できます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、MAC アドレスを指定します。各 MAC アドレスのフォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字（0 ～ 9、A ～ F、または a ～ f）です。MAC アドレスは、1 つ以上の空白スペースで区切る必要があります。

MAC アドレスによって個々のシステムが区別されるので、特定のデバイスに対するポリシーを設定できます。システムの MAC アドレスを取得するには、そのデバイスを ASA に接続して DAP トレースを実行し、**endpoint.anyconnect.macaddress** の値を見つける必要があります。この値を [MAC Address Pool] フィールドに入力する必要があります。

ステップ 8　[OK] をクリックします。

DAP へのファイル エンドポイント属性の追加

はじめる前に

ファイル エンドポイント属性を設定する前に、どのファイルをスキャンするかを Cisco Secure Desktop の [Host Scan] ウィンドウで定義します。ASDM で、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] を選択します。詳細については、そのページの [Help] をクリックします。

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [File] を選択します。

ステップ 2　[Exists] と [Does not exist] のオプション ボタンでは、選択したエンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものを選択します。

ステップ 3　[Endpoint ID] リスト ボックスで、スキャン対象のファイル エントリに等しいエンドポイント ID をドロップダウン リストから選択します。

ファイルの情報が [Endpoint ID] リスト ボックスの下に表示されます。

ステップ 4　[Last Update] チェックボックスをオンにしてから、更新日からの日数が指定の値よりも小さい（<）と大きい（>）のどちらを条件とするかを操作フィールドで選択します。更新日からの日数を [days] フィールドに入力します。

ステップ 5　[Checksum] チェックボックスをオンにしてから、テスト対象ファイルのチェックサム値と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 6　[Compute CRC32 Checksum] をクリックすると、テスト対象のファイルのチェックサム値が計算されます。

ステップ 7　[OK] をクリックします。

DAP へのデバイス エンドポイント属性の追加

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [Device] を選択します。

ステップ 2　[Host Name] チェックボックスをオンにしてから、テスト対象デバイスのホスト名と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。完全修飾ドメイン名（FQDN）ではなく、コンピュータのホスト名のみを使用します。

ステップ 3　[MAC address] チェックボックスをオンにしてから、テスト対象のネットワーク インターフェイス カードの MAC アドレスと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。1 つのエントリにつき MAC アドレスは 1 つだけです。アドレスのフォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。

ステップ 4　[BIOS Serial Number] チェックボックスをオンにしてから、テスト対象のデバイスの BIOS シリアル番号と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。数値フォーマットは、製造業者固有です。フォーマット要件はありません。

ステップ 5　[TCP/UDP Port Number] チェックボックスをオンにしてから、テスト対象のリスニング状態の TCP ポートと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

TCP/UDP コンボ ボックスでは、テスト対象（TCP（IPv4）、UDP（IPv4）、TCP（IPv6）、または UDP（IPv6））のポートの種類を選択します。複数のポートをテストする場合は、DAP の個々のエンドポイント属性のルールをいくつか作成し、それぞれに 1 個のポートを指定します。

ステップ 6　[Version of Secure Desktop (CSD)] チェックボックスをオンにしてから、エンドポイント上で実行されるホスト スキャン イメージのバージョンと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 7　[Version of Endpoint Assessment] チェックボックスをオンにしてから、テスト対象のエンドポイント アセスメント（OPSWAT）のバージョンと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 8　[OK] をクリックします。

DAP への NAC エンドポイント属性の追加

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [NAC] を選択します。

ステップ 2　[Posture Status] チェックボックスをオンにしてから、ACS によって受信されるポスチャ トークン文字列と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。ポスチャ トークン文字列を [Posture Status] テキスト ボックスに入力します。

ステップ 3　[OK] をクリックします。

DAP へのオペレーティング システム エンドポイント属性の追加

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [Operating System] を選択します。

ステップ 2　[OS Version] チェックボックスをオンにしてから、[OS Version] リスト ボックスで設定するオペレーティング システム（Windows、Mac、または Linux）と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 3　[OS Update] チェックボックスをオンにしてから、[OS Update] テキスト ボックスに入力する Windows、Mac、または Linux オペレーティング システムのサービス パックと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 4　[OK] をクリックします。

DAP へのパーソナル ファイアウォール エンドポイント属性の追加

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [Operating System] を選択します。

ステップ 2　適切なボタン [Enabled]、[Disabled]、または [Not Installed] をクリックして、選択したエンドポイント属性とそれに付随する修飾子（[Enabled]/[Disabled]/[Not Installed] ボタンの下のフィールド）をイネーブルにするか、ディセーブルにするか、またはインストールしないかを指定します。

ステップ 3　[Vendor ID] リスト ボックスで、テスト対象のパーソナル ファイアウォール ベンダーの名前をクリックします。

ステップ 4　[Product Description] チェックボックスをオンにして、テストするベンダーの製品名をリスト ボックスから選択します。

ステップ 5　[Version] チェックボックスをオンにして、操作フィールドを、[Version] リスト ボックスで選択した製品バージョン番号に等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）に設定します。

[Version] リスト ボックスで選択したバージョンに x が付いている場合（たとえば 3.x）は、この x を具体的なリリース番号で置き換えます（たとえば 3.5）。

ステップ 6　[OK] をクリックします。

DAP へのポリシー エンドポイント属性の追加

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [Policy] を選択します。

ステップ 2　[Location] チェックボックスをオンにしてから、Cisco Secure Desktop Microsoft Windows ロケーション プロファイルと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。Cisco Secure Desktop Microsoft Windows ロケーション プロファイル文字列を [Location] テキスト ボックスに入力します。

ステップ 3　[OK] をクリックします。

DAP へのプロセス エンドポイント属性の追加

はじめる前に

プロセス エンドポイント属性を設定する前に、どのプロセスをスキャンするかを Cisco Secure Desktop の [Host Scan] ウィンドウで定義します。ASDM で、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] を選択します。詳細については、そのページの [Help] をクリックします。

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [Process] を選択します。

ステップ 2　[Exists] または [Does not exist] のボタンでは、選択したエンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものをクリックします。

ステップ 3　[Endpoint ID] リスト ボックスで、スキャン対象のエンドポイント ID をドロップダウン リストから選択します。

エンドポイント ID プロセス情報がリスト ボックスの下に表示されます。

ステップ 4　[OK] をクリックします。

DAP へのレジストリ エンドポイント属性の追加

レジストリ エンドポイント属性のスキャンは Windows オペレーティング システムにのみ適用されます。

はじめる前に

レジストリ エンドポイント属性を設定する前に、どのレジストリ キーをスキャンするかを Cisco Secure Desktop の [Host Scan] ウィンドウで定義します。ASDM で、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] を選択します。詳細については、そのページの [Help] をクリックします。

ステップ 1　[Endpoint Attribute Type] リスト ボックスで [Registry] を選択します。

ステップ 2　[Exists] または [Does not exist] のボタンでは、レジストリ エンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものをクリックします。

ステップ 3　[Endpoint ID] リスト ボックスで､スキャン対象のレジストリ エントリに等しいエンドポイント ID をドロップダウン リストから選択します。

レジストリの情報が [Endpoint ID] リスト ボックスの下に表示されます。

ステップ 4　[Value] チェックボックスをオンにしてから、操作フィールドで等しい（=）または等しくない（!=）を選択します。

ステップ 5　最初の [Value] リスト ボックスで、レジストリ キーが dword か文字列かを指定します。

ステップ 6　2 つ目の [Value] 操作リスト ボックスに、スキャン対象のレジストリ キーの値を入力します。

ステップ 7　スキャン時にレジストリ エントリの大文字と小文字の違いを無視するには、チェックボックスをオンにします。検索時に大文字と小文字を区別するには、チェックボックスをオフにしてください。

ステップ 8　[OK] をクリックします。

DAP とアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラム

セキュリティ アプライアンスは、ユーザ属性が、設定済みの AAA 属性およびエンドポイント属性に一致する場合に DAP ポリシーを使用します。Cisco Secure Desktop のプリログイン評価モジュールおよびホスト スキャン モジュールは、設定済みエンドポイント属性の情報をセキュリティ アプライアンスに返し、DAP サブシステムでは、その情報に基づいてそれらの属性値に一致する DAP レコードを選択します。

アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラムのほとんど（すべてではなく）は、アクティブ スキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。ホスト スキャンは、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを、次のようにしてチェックします。

- インストールされているプログラムがアクティブ スキャンをサポートしない場合、ホスト スキャンはそのソフトウェアの存在をレポートします。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがイネーブルになっている場合、ホスト スキャンはそのソフトウェアの存在をレポートします。この場合も、セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがディセーブルになっている場合、ホスト スキャンはそのソフトウェアの存在を無視します。セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択しません。さらに、そのプログラムがインストールされているとしても、DAP についての情報が多く含まれる **debug trace** コマンドの出力にはプログラムの存在が示されません。

エンドポイント属性の定義

次に、DAP で使用できるエンドポイント選択属性を示します。属性名フィールドは、Lua 論理式での各属性名の入力方法を示しており、[Dynamic Access Policy Selection Criteria] ペインの [Advanced] 領域で使用します。*label* 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
アンチスパイウェア（Cisco Secure Desktop が必要）	endpoint.as["*label*"].exists	ホスト スキャン	true	—	アンチスパイウェア プログラムが存在する
	endpoint.as["*label*"].version		ストリング	32	バージョン
	endpoint.as["*label*"].description		ストリング	128	アンチスパイウェアの説明
	endpoint.as["*label*"].lastupdate		整数	—	アンチスパイウェア定義を更新してからの経過時間（秒）

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
ウイルス対策 （Cisco Secure Desktop が必要）	endpoint.av["*label*"].exists	ホストスキャン	true	—	アンチウイルス プログラムが存在する
	endpoint.av["*label*"].version		ストリング	32	バージョン
	endpoint.av["*label*"].description		ストリング	128	アンチウイルスの説明
	endpoint.av["*label*"].lastupdate		整数	—	アンチウイルス定義を更新してからの経過時間（秒）
AnyConnect （Cisco Secure Desktop やホスト スキャンは必要ありません）	endpoint.anyconnect.clientversion	エンドポイント	version	—	AnyConnect クライアントのバージョン。
	endpoint.anyconnect.platform		ストリング	—	AnyConnect クライアントがインストールされているオペレーティング システム。
	endpoint.anyconnect.platformversion		version	64	AnyConnect クライアントがインストールされているオペレーティング システムのバージョン。
	endpoint.anyconnect.devicetype		ストリング	64	AnyConnect クライアントがインストールされているモバイル デバイスのタイプ。
	endpoint.anyconnect.deviceuniqueid			64	AnyConnect クライアントがインストールされているモバイル デバイスの一意の ID。
	endpoint.anyconnect.macaddress		ストリング	フォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字です。	AnyConnect クライアントがインストールされているデバイスの MAC アドレス。
アプリケーション	endpoint.application.clienttype	アプリケーション	ストリング	—	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
デバイス	endpoint.device.hostname	エンドポイント	ストリング	64	ホスト名のみ。FQDN ではありません。
	endpoint.device.MAC		ストリング	フォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。	ネットワーク インターフェイス カードの MAC アドレス。1 つのエントリにつき MAC アドレスは 1 つだけです。
	endpoint.device.id		ストリング	64	BIOS シリアル番号。数値フォーマットは、製造業者固有です。フォーマット要件はありません。
	endpoint.device.port		ストリング	1 ～ 65535 の整数。	リスニング状態の TCP ポート。1 回線ごとに 1 つのポートを定義できます。
	endpoint.device.protection_version		ストリング	64	実行されるホスト スキャン イメージのバージョン。
	endpoint.device.protection_extension		ストリング	64	Endpoint Assessment（OPSWAT）のバージョン
ファイル	endpoint.file["*label*"].exists	Secure Desktop	true	—	ファイルが存在する
	endpoint.file[“label”].endpointid				
	endpoint.file["*label*"].lastmodified		整数	—	ファイルが最後に変更されてからの経過時間（秒）
	endpoint.file["*label*"].crc.32		整数	—	ファイルの CRC32 ハッシュ
NAC	endpoint.nac.status	NAC	ストリング	—	ユーザ定義ステータス ストリング
オペレーティング システム	endpoint.os.version	Secure Desktop	ストリング	32	オペレーティング システム
	endpoint.os.servicepack		整数	—	Windows のサービス パック
パーソナル ファイアウォール（Secure Desktop が必要）	endpoint.fw["*label*"].exists	ホスト スキャン	true	—	パーソナル ファイアウォールが存在する
	endpoint.fw["*label*"].version		ストリング	32	バージョン
	endpoint.fw["*label*"].description		ストリング	128	パーソナル ファイアウォールの説明

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
ポリシー	endpoint.policy.location	Secure Desktop	ストリング	64	Cisco Secure Desktop からのロケーション値
プロセス	endpoint.process["*label*"].exists	Secure Desktop	true	—	プロセスが存在する
	endpoint.process["*label*"].path		ストリング	255	プロセスのフル パス
レジストリ	endpoint.registry["*label*"].type	Secure Desktop	*dword ストリング*	—	dword
	endpoint.registry["*label*"].value		ストリング	255	レジストリ エントリの値
VLAN	endoint.vlan.type	CNA	ストリング	—	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

Lua を使用した DAP における追加の DAP 選択基準の作成

この項では、AAA またはエンドポイント属性の論理式の作成方法について説明します。これを行うには、Lua に関する高度な知識が必要です。Lua のプログラミングについての詳細は、以下を参照してください。http://www.lua.org/manual/5.1/manual.html

[Advanced] フィールドに、AAA またはエンドポイント選択論理演算を表す自由形式の Lua テキストを入力します。ASDM は、ここで入力されるテキストを検証せず、このテキストを単に DAP ポリシー ファイルにコピーするだけです。ASA がそれを処理し、解析不能な式があれば破棄されます。

このオプションは、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。たとえば、指定された条件のいずれかまたはすべてを満たす、あるいはいずれも満たさない AAA 属性を使用するように ASA を設定できます。エンドポイント属性は累積され、すべて満たす必要があります。セキュリティ アプライアンスで 1 つのエンドポイント属性または別の属性を使用できるようにするには、Lua で適切な論理式を作成してここで入力する必要があります。

次の各項では、Lua EVAL 式作成の詳細と、例を示します。

- 「Lua EVAL 式を作成する構文」
- 「DAP CheckAndMsg 関数」
- 「DAP EVAL 式の例」
- 「追加の Lua 機能」

Lua EVAL 式を作成する構文

（注）　[Advanced] モードを使用する必要がある場合は、プログラムを直接的に検証することが可能になり、明確になるため、できるだけ EVAL 式を使用することをお勧めします。

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA 属性、または Cisco Secure Desktop から返された属性。属性の定義については、「エンドポイント属性の定義」（P.5-16）を参照してください。	
<comparison>	次の文字列のいずれか（引用符が必要）	
	“EQ”	等しい
	“NE”	等しくない
	“LT”	より小さい
	“GT”	より大きい
	“LE”	以下
	“GE”	以上
<value>	引用符で囲まれ、属性と比較する値を含む文字列	
<type>	次の文字列のいずれか（引用符が必要）	
	“string”	大文字、小文字を区別する文字列の比較
	“”	大文字、小文字を区別しない文字列の比較
	“integer”	数値比較で、文字列値を数値に変換
	“hex”	16 進数を用いた数値比較で、16 進数の文字列を 16 進数に変換
	“version”	X.Y.Z の形式でバージョンを比較 （X、Y、Z はいずれも数値）

DAP CheckAndMsg 関数

CheckAndMsg は、DAP がコールするように設定可能な Lua 関数です。条件に基づきユーザ メッセージを生成します。

DAP の [Advanced] フィールドで、CheckAndMsg を使用するように ASDM を設定できます。ASA は、Lua CheckAndMsg 関数が選択されており、結果がクライアントレス SSL VPN または AnyConnect のターミネーションとなるときだけに、メッセージをユーザに表示します。

CheckAndMsg 関数の構文は以下のとおりです。

```
CheckAndMsg(value, “<message string if value is true>”, “<message string if value if false>”)
```

CheckAndMsg 関数の作成時には、以下の点に注意してください。

- CheckAndMsg は、最初の引数として渡された値を返します。
- 文字列比較を使用したくない場合、EVAL 関数を最初の引数として使用してください。次に例を示します。

```
(CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
```

CheckandMsg は EVAL 関数の結果を返し、セキュリティ アプライアンスは DAP レコードを選択すべきかどうかを判断するのにその結果を使用します。レコードが選択された結果、ターミネーションとなった場合、セキュリティ アプライアンスは適切なメッセージを表示します。

DAP EVAL 式の例

Lua で論理式を作成する場合は、これらの例を参考にしてください。

説明	例
Windows XP かどうかをテストするエンドポイント。	`EVAL(endpoint.os.version, "EQ", "Windows XP", "string")`
CLIENTLESS または CVC クライアント タイプに一致するかどうかをテストするエンドポイント式。	`(EVAL(endpoint.application.clienttype,"EQ","CLIENTLESS") or EVAL(endpoint.application.clienttype, "EQ","CVC"))`
Norton Antivirus バージョン 10.x かどうかをテストするが、10.5.x は除外するエンドポイント式。	`(EVAL(endpoint.av["NortonAV"].version, "GE", "10","version") and EVAL(endpoint.av["NortonAV"].version,"LT", "10.5", "version") or EVAL(endpoint.av["NortonAV"].version, "GE", "10.6", "version")))`
単一アンチウイルス プログラム McAfee がユーザの PC にインストールされているかどうかのチェック。インストールされていない場合はメッセージを表示します。	`(CheckAndMsg(EVAL(endpoint.av["McAfeeAV"].exists,"NE","true") ,"McAfee AV was not found on your computer", nil))`
McAfee アンチウイルス定義が過去 10 日（864000 秒）以内に更新されたかどうかのチェック。更新が必要な場合はメッセージを表示します。	`((CheckAndMsg(EVAL(endpoint.av["McAfeeAV"].lastupdate,"GT", "864000","integer"),"AV Update needed!Please wait for the McAfee AV till it loads the latest dat file.",nil) ))`
debug dap trace で以下が返された後に特定のホットフィックスがあるかどうかをチェック。 `endpoint.os.windows.hotfix ["KB923414"] = "true";`	`(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"], "NE","true"),"The required hotfix is not installed on your PC.",nil))`

アンチウイルス プログラムのチェック

アンチウイルス プログラムがない場合、または実行していない場合も、ユーザが問題に気づき、修正できるようにメッセージを設定できます。これにより、アクセスが拒否されても、ASA は「ターミネーション」状態の原因となったすべてのメッセージを DAP から収集し、ブラウザのログイン ページに表示します。アクセスが許可された場合、ASA はポータル ページの DAP 評価プロセスで生成されたすべてのメッセージを表示します。

次の例は、Norton Antivirus プログラムのチェックでこの機能を使用する方法を示します。

1. 次の Lua 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます（右端にある二重矢印をクリックして、フィールドを展開します）。

```
(CheckAndMsg(EVAL(endpoint.av["NortonAV"].exists, "EQ", "false"),"Your Norton AV was found
but the active component of it was not enabled", nil) or
CheckAndMsg(EVAL(endpoint.av["NortonAV"].exists, "NE", "true"),"Norton AV was not found on
your computer", nil) )
```

2. 同じ [Advanced] フィールドで、[OR] ボタンをクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Norton Antivirus がインストールされていないか、無効になっている PC から接続します。予測される結果は、接続が許可されず、かつメッセージが点滅する !で表示されます。
5. 点滅する！をクリックして、メッセージを表示します。

アンチウイルス プログラムと、1 日半以上経過した定義のチェック

この例では、Norton または McAfee のアンチウイルス プログラムが存在するかどうか、また、ウイルス定義が 1 日半（10,000 秒）以内のものであるかどうかを確認します。定義が 1 日半以上経過している場合、ASA はセッションを終了し、メッセージと、修正するためのリンクを表示します。このタスクを完了するには、次の手順を実行します。

1. 次の Lua 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます（右端にある二重矢印をクリックして、フィールドを展開します）。

```
((EVAL(endpoint.av["NortonAV"].exists,"EQ","true","string") and
CheckAndMsg(EVAL(endpoint.av["NortonAV"].lastupdate,"GT","10000",integer"),To remediate <a
href='http://www.symantec.com'>Click this link </a>",nil)) or
(EVAL(endpoint.av["McAfeeAV"].exists,"EQ","true","string") and
CheckAndMsg(EVAL(endpoint.av["McAfeeAV"].lastupdate,"GT","10000",integer"),To remediate <a
href='http://www.mcafee.com'>Click this link</a>",nil))
```

2. 同じ [Advanced] フィールドで、[AND] をクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Norton または McAfee のアンチウイルス プログラムがインストールされており、バージョンが 1 日半以上前のものである PC から 接続します。予測される結果は、接続が許可されず、かつメッセージが点滅する !で表示されます。
5. 点滅する！をクリックして、メッセージと、修復のためのリンクを表示します。

追加の Lua 機能

クライアントレス SSL VPN のダイナミック アクセス ポリシーで作業している場合、一致基準に高度な柔軟性が必要とされることが考えられます。たとえば、以下に従い別の DAP を適用しなければならない場合があります。

- 組織ユニット（OU）またはユーザ オブジェクトの他の階層のレベル
- 命名規則に従っているものの、一致する可能性が高いグループ名。グループ名ではワイルドカードを使用したほうが良い場合があります。

ASDM の [DAP] ペイン内の [Advanced] セクションで Lua 論理式を作成し、この柔軟性を実現できます。

OU ベースの一致例

DAP は、論理式で LDAP サーバから返される多数の属性を使用できます。DAP トレースの項で出力例を参照するか、debug dap trace を実行してください。

LDAP サーバはユーザの認定者名（DN）を返します。これは、ディレクトリ内のどの部分にユーザ オブジェクトがあるかを暗黙的に示します。たとえば、ユーザの DN が CN=Example User,OU=Admins,dc=cisco,dc=com である場合、このユーザは OU=Admins,dc=cisco,dc=com に存在します。すべての管理者がこの OU（または、このレベル以下のコンテナ）に存在する場合、以下のように、この基準に一致する論理式を使用できます。

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) )
then
       return true
   end
   return false
end)()
```

この例では、string.find 関数で正規表現を使用できます。文字列の最後に $ を使用し、この文字列から distinguishedName フィールドの最後へのアンカーをつけます。

グループ メンバーシップの例

AD グループ メンバーシップのパターン照合のために、基本論理式を作成できます。ユーザが複数のグループのメンバーであることが考えられるため、DAP は LDAP サーバからの応答を表内の別々のエントリへと解析します。以下を実行するには、高度な機能が必要です。

- memberOf フィールドを文字列として比較する（ユーザが 1 つのグループだけに所属している場合）。
- 返されたそれぞれの memberOf フィールドで繰り返し処理し、返されたデータが「table」タイプであるかどうかを確認する。

そのために記述し、テストした関数を以下に示します。この例では、ユーザが「-stu」で終わるいずれかのグループのメンバーである場合、この DAP に一致します。

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

アンチウイルスの例

次の例は、アンチウイルス ソフトウェアが検知されたかどうかを確認するためにカスタム関数を使用しています。

```
assert(function()
    for k,v in pairs(endpoint.av) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

アンチスパイウェアの例

次の例は、アンチスパイウェアが検知されたかどうかを確認するためにカスタム関数を使用しています。

```
assert(function()
    for k,v in pairs(endpoint.as) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

ファイアウォールの例

次の例は、ファイアウォールが検知されたかどうかを確認するためにカスタム関数を使用しています。

```
assert(function()
    for k,v in pairs(endpoint.fw) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

アンチウイルス、アンチスパイウェア、*または*すべてのファイアウォールの例

次の例は、アンチウイルス、アンチスパイウェアまたはファイアウォールのいずれかの存在が検知されたかどうかを確認するためにカスタム関数を使用しています。

```
assert(function()
       function check(antix)
           if (type(antix) == "table") then
               for k,v in pairs(antix) do
                   if (EVAL(v.exists, "EQ", "true", "string")) then
                       return true
                   end
               end
           end
           return false
       end
       return (check(endpoint.av) or check(endpoint.fw) or check(endpoint.as))
   end)()
```

アクセス拒否の例

アンチウイルス プログラムが存在しない場合のアクセスを拒否するために、次の関数を使用できます。ターミネーションを実行するためのアクションが設定されている DAP で使用します。

```
assert( function()
for k,v in pairs(endpoint.av) do
    if (EVAL(v.exists, "EQ", "true", "string")) then
        return false
    end
    end
    return CheckAndMsg(true, "Please install antivirus software before connecting.", nil)
end)()
```

アンチウイルス プログラムがないユーザがログインしようとすると、DAP は次のメッセージを表示します。

```
Please install antivirus software before connecting.
```

DAP アクセスと許可ポリシー属性の設定

次の各タブをクリックして、タブ内のフィールドを設定します。

[Action] タブ

特定の接続またはセッションに適用する特殊な処理を指定します。

- [Continue]：（デフォルト）セッションにアクセス ポリシー属性を適用します。
- [Quarantine]：検疫を使用すると、すでに VPN 経由でトンネルを確立した特定のクライアントを制限できます。ASA は、制限付き ACL をセッションに適用して制限付きグループを形成します。この基になるのは、選択された DAP レコードです。管理目的で定義されたポリシーにエンドポイントが準拠していないときも、ユーザは修復のためのサービス（たとえばアンチウイルス アプリケーションのアップデート）にアクセスできますが、そのユーザには制限が適用されます。修復後、ユーザは再接続できます。この再接続により、新しいポスチャ アセスメントが起動されます。このアセスメントに合格すると、接続されます。このパラメータを使用するには、AnyConnect セキュア モビリティ機能をサポートしている AnyConnect リリースが必要です。
- [Terminate]：セッションを終了します。
- [User Message]：この DAP レコードが選択されるときに、ポータル ページに表示するテキスト メッセージを入力します。最大 490 文字です。ユーザ メッセージは、黄色のオーブとして表示されます。ユーザがログインすると、メッセージは 3 回点滅してから静止します。数件の DAP レコードが選択され、それぞれにユーザ メッセージがある場合は、ユーザ メッセージがすべて表示されます。

  URL やその他の埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必要があります。例：すべてのコントラクタは、ご使用のアンチウイルス ソフトウェアのアップグレード手順について、 Instructions を参照してください。

[Network ACL Filters] タブ

この DAP レコードに適用するネットワーク ACL を選択および設定できます。DAP の ACL には、許可ルールまたは拒否ルールを含めることができますが、両方を含めることはできません。ACL に許可ルールと拒否ルールの両方が含まれている場合、ASA はその ACL を拒否します。

- [Network ACL] ドロップダウン リスト：この DAP レコードに追加する、設定済みのネットワーク ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。このフィールドは、IPv4 および IPv6 ネットワーク トラフィックのアクセス ルールを定義できる統合 ACL をサポートしています。
- [Manage...]：ネットワーク ACL を追加、編集、および削除するときにクリックします。
- [Network ACL] リスト：この DAP レコードのネットワーク ACL が表示されます。
- [Add>>]：クリックすると、ドロップダウン リストで選択したネットワーク ACL が右側の [Network ACLs] リストに追加されます。
- [Delete]：クリックすると、強調表示されているネットワーク ACL が [Network ACLs] リストから削除されます。ASA から ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

[Web-Type ACL Filters (clientless)] タブ

この DAP レコードに適用する Web タイプ ACL を選択および設定できます。DAP の ACL には、許可または拒否ルールだけを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれている場合、ASA はその ACL を拒否します。

- [Web-Type ACL] ドロップダウン リスト：この DAP レコードに追加する、設定済みの Web タイプ ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。
- [Manage...]：Web タイプ ACL を追加、編集、および削除するときにクリックします。
- [Web-Type ACL] リスト：この DAP レコードの Web タイプ ACL が表示されます。
- [Add>>]：クリックすると、ドロップダウン リストで選択した Web タイプ ACL が右側の [Web-Type ACLs] リストに追加されます。
- [Delete]：クリックすると、Web タイプ ACL の 1 つが [Web-Type ACLs] リストから削除されます。ASA から ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

[Functions] タブ

DAP レコードのファイル サーバ入力とブラウジング、HTTP プロキシ、および URL 入力を設定できます。

- [File Server Browsing]：ファイル サーバまたは共有機能の CIFS ブラウジングをイネーブルまたはディセーブルにします。

  ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。CIFS ブラウズ機能では、国際化がサポートされていません。
- [File Server Entry]：ポータル ページでユーザがファイル サーバのパスおよび名前を入力できるようにするかどうかを設定します。イネーブルになっている場合、ポータル ページにファイル サーバ エントリのドロワが配置されます。ユーザは、Windows ファイルへのパス名を直接入力できます。ユーザは、ファイルをダウンロード、編集、削除、名前変更、および移動できます。また、ファイルおよびフォルダを追加することもできます。適用可能な Windows サーバでユーザ アクセスに対して共有を設定する必要もあります。ネットワークの要件によっては、ユーザがファイルへのアクセス前に認証を受ける必要があることもあります。
- [HTTP Proxy]：クライアントへの HTTP アプレット プロキシの転送に関与します。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
- [URL Entry]：ポータル ページでユーザが HTTP/HTTPS URL を入力できるようにするかどうかを設定します。この機能がイネーブルになっている場合、ユーザは URL エントリ ボックスに Web アドレスを入力できます。また、クライアントレス SSL VPN を使用して、これらの Web サイトにアクセスできます。

SSL VPN を使用しても、すべてのサイトとの通信が必ずしもセキュアになるとは限りません。SSL VPN は、企業ネットワーク上のリモート ユーザの PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信はセキュアではありません。

クライアントレス VPN 接続では、ASA はエンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。ユーザが SSL 対応 Web サーバに接続すると、ASA はセキュアな接続を確立し、SSL 証明書を検証します。エンド ユーザ ブラウザでは提示された証明書を受信しないため、証明書を調査して検証することはできません。SSL VPN の現在の実装では、期限切れになった証明書を提示するサイトとの通信は許可されません。また、ASA は、信頼できる CA 証明書の検証も実行しません。このため、ユーザは、SSL 対応の Web サーバと通信する前に、そのサーバにより提示された証明書を分析することはできません。

ユーザのインターネット アクセスを制限するには、[Disable for the URL Entry] フィールドを選択します。これにより、SSL VPN ユーザがクライアントレス VPN 接続中に Web サーフィンできないようにします。

- [Unchanged]：（デフォルト）クリックすると、このセッションに適用されるグループ ポリシーからの値が使用されます。
- [Enable/Disable]：機能をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックすると HTTP プロキシがイネーブルになり、これらの機能に関連付けられたアプレットが DAP レコードによって自動的に起動するようになります。

[Port Forwarding Lists] タブ

ユーザ セッションのためのポート転送リストを選択および設定できます。

ポート転送によりグループ内のリモート ユーザは、既知の固定 TCP/IP ポートで通信するクライアント/サーバ アプリケーションにアクセスできます。リモート ユーザは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモート サーバに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP（FTP over SSH）、Perforce、Outlook Express、および Lotus Notes についてテストしています。その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、シスコではテストしていません。

（注） ポート転送は、一部の SSL/TLS バージョンでは使用できません。

注意 ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートする Sun Microsystems Java Runtime Environment（JRE）1.4+ がリモート コンピュータにインストールされていることを確認します。

- [Port Forwarding]：この DAP レコードに適用されるポート転送リストのオプションを選択します。このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Auto-start] に設定した場合にだけイネーブルになります。
- [Unchanged]：クリックすると、属性が実行コンフィギュレーションから削除されます。
- [Enable/Disable]：ポート転送をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックするとポート転送がイネーブルになり、DAP レコードのポート転送リストに関連付けられたポート転送アプレットが自動的に起動するようになります。

- [Port Forwarding List] ドロップダウン リスト：DAP レコードに追加する、設定済みのポート転送リストを選択します。
- [New...]：新規のポート転送リストを設定するときにクリックします。
- [Port Forwarding Lists]（ラベルなし）：DAP レコードのポート転送リストが表示されます。
- [Add]：クリックすると、ドロップダウン リストで選択したポート転送リストが右側のポート転送リストに追加されます。
- [Delete]：クリックすると、選択されているポート転送リストがポート転送リストから削除されます。ASA からポート転送リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。

[Bookmarks] タブ

特定のユーザ セッション URL のブックマークを選択および設定できます。

- [Enable bookmarks]：クリックするとイネーブルになります。このチェックボックスがオフのときは、接続のポータル ページにブックマークは表示されません。
- [Bookmark] ドロップダウン リスト：DAP レコードに追加する、設定済みのブックマークを選択します。
- [Manage...]：ブックマークを追加、インポート、エクスポート、削除するときにクリックします。
- [Bookmarks]（ラベルなし）：この DAP レコードの URL リストが表示されます。
- [Add>>]：クリックすると、ドロップダウン リストで選択したブックマークが右側の URL 領域に追加されます。
- [Delete]：クリックすると、選択されているブックマークが URL リスト領域から削除されます。ASA からブックマークを削除するには、まず DAP レコードからそのブックマークを削除する必要があります。

[Access Method] タブ

許可するリモート アクセスのタイプを設定できます。

- [Unchanged]：現在のリモート アクセス方式を引き続き使用します。
- [AnyConnect Client]：Cisco AnyConnect VPN クライアントを使用して接続します。
- [Web-Portal]：クライアントレス VPN で接続します。
- [Both-default-Web-Portal]：クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトはクライアントレスです。
- [Both default AnyConnect Client]：クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトは AnyConnect です。

[AnyConnect] タブ

Always-on VPN フラグのステータスを選択できます。

- [Always-On VPN for AnyConnect client] : AnyConnect サービス プロファイル内の Always-on VPN フラグ設定を未変更にするか、ディセーブルにするか、AnyConnect プロファイル設定を使用するかを指定します。

  このパラメータを使用するには、Cisco IronPort Web セキュリティ アプライアンスのリリースが、Cisco AnyConnect VPN クライアントに対してセキュア モビリティ ソリューション ライセンシングをサポートしている必要があります。また、AnyConnect のリリースが、「セキュア モビリティ ソリューション」の機能をサポートしている必要もあります。詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

[AnyConnect Custom Attributes] タブ

このポリシーに現在割り当てられているカスタム属性を示します。このダイアログボックスでは、すでに定義済みのカスタム属性をこのポリシーに関連付けるか、カスタム属性を定義してこのポリシーに関連付けることができます。

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

カスタム属性は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] および [AnyConnect Custom Attribute Names] で事前に定義できます。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。

カスタム属性の設定手順は両方のタイプのポリシーで同じであるため、この手順については「内部グループ ポリシーの AnyConnect クライアント カスタム属性について」（P.3-22）を参照してください。

DAP トレースの実行

DAP トレースを実行すると、すべての接続済みデバイスの DAP エンドポイント属性が表示されます。

ステップ 1　SSH ターミナルから ASA にログオンして特権 EXEC モードを開始します。

ASA の特権 EXEC モードでは、表示されるプロンプトは `hostname#` となります。

ステップ 2　DAP デバッグをイネーブルにします。セッションのすべての DAP 属性がターミナル ウィンドウに表示されます。

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

ステップ 3　（オプション）DAP トレースの出力を検索するには、コマンドの出力をシステム ログに送ります。ASA でのロギングの詳細については、『*Cisco ASA Series General Operations ASDM Configuration Guide*』の「*Configure Logging*」を参照してください。

DAP の例

DAP を使用したネットワーク リソースの定義

この例は、ユーザまたはグループのネットワーク リソースを定義する方法として、ダイナミック アクセス ポリシーを設定する方法を示しています。Trusted_VPN_Access という名前の DAP ポリシーは、クライアントレス VPN アクセスと AnyConnect VPN アクセスを許可します。Untrusted_VPN_Access という名前のポリシーは、クライアントレス VPN アクセスだけを許可します。

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [Endpoint] に移動し、ポリシーごとに次の属性を設定します。

属性	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	信頼できる	信頼できない
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	信頼できる	信頼できない
LDAP memberOf	Engineering、Managers	ベンダー
ACL		Web-Type ACL
Access	**AnyConnect** *および* **Web Portal**	**Web Portal**

DAP を使用した WebVPN ACL の適用

DAP では、Network ACLs（IPsec および AnyConnect の場合）、Clientless SSL VPN Web-Type ACLs、URL リスト、および Functions を含め、アクセス ポリシー属性のサブセットを直接適用できます。グループ ポリシーが適用されるバナーまたはスプリット トンネル リストなどには、直接適用できません。[Add/Edit Dynamic Access Policy] ペインの [Access Policy Attributes] タブには、DAP が直接適用される属性の完全なメニューが表示されます。

Active Directory/LDAP は、ユーザ グループ ポリシー メンバーシップをユーザ エントリの「memberOf」属性として保存します。DAP は、AD グループ（memberOf）のユーザ = ASA が設定済み Web タイプ ACL を適用する Engineering となるように定義します。

ステップ 1　ASDM で、[Add AAA Attributes] ペイン（[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [AAA Attributes] セクション > [Add AAA Attribute]）に移動します。

ステップ 2　AAA 属性タイプとしては、ドロップダウン リストを使用して [LDAP] を選択します。

ステップ 3　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4　[Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Engineering」と入力します。

ステップ 5　ペインの [Access Policy Attributes] 領域で、[Web-Type ACL Filters] タブをクリックします。

ステップ 6　[Web-Type ACL] ドロップダウン リストを使用して、AD グループ（memberOf）= Engineering のユーザに適用する ACL を選択します。

CSD チェックの強制と DAP によるポリシーの適用

この例では、ユーザが 2 つの特定 AD/LDAP グループ（Engineering および Employees）と 1 つの特定 ASA トンネル グループに属することをチェックする DAP を作成します。その後、ACL をユーザに適用します。

DAP が適用される ACL により、リソースへのアクセスを制御します。それらの ACL は、ASA のグループ ポリシーで定義されるどの ACL よりも優先されます。また ASA は、スプリット トンネリング リスト、バナー、および DNS など、DAP で定義または制御しない要素の通常の AAA グループ ポリシー継承ルールおよび属性を適用します。

ステップ 1　ASDM で、[Add AAA Attributes] ペイン（[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [AAA Attributes] セクション > [Add AAA Attribute]）に移動します。

ステップ 2　AAA 属性タイプとしては、ドロップダウン リストを使用して [LDAP] を選択します。

ステップ 3　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4　[Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Engineering」と入力します。

ステップ 5　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 6　[Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Employees」と入力します。

ステップ 7　AAA 属性タイプとしては、ドロップダウン リストを使用して [Cisco] を選択します。

ステップ 8　[Tunnel] グループ ボックスをオンにし、ドロップダウン リストを使用して [=] を選択し、隣のドロップダウン リストで適切なトンネル グループ（接続ポリシー）を選択します。

ステップ 9　[Access Policy Attributes] 領域の [Network ACL Filters] タブで、前のステップで定義した DAP 基準を満たすユーザに適用する ACL を選択します。

CHAPTER 6

電子メール プロキシ

電子メール プロキシを設定すると、リモート電子メール機能をクライアントレス SSL VPN のユーザに拡張できます。ユーザが電子メール プロキシ経由で電子メール セッションを試行すると、電子メール クライアントが SSL プロトコルを使用してトンネルを確立します。

電子メール プロキシ プロトコルは次のとおりです。

POP3S

POP3S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 995 をリッスンし、ポート 995 または設定されたポートとの接続が自動的に許可されます。POP3 プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に POP3 プロトコルが開始され、認証が行われます。POP3S は、電子メール受信用のプロトコルです。

IMAP4S

IMAP4S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 993 をリッスンし、ポート 993 または設定されたポートとの接続が自動的に許可されます。IMAP4S プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に IMAP4S プロトコルが開始され、認証が行われます。IMAP4S は、電子メール受信用のプロトコルです。

SMTPS

SMTPS は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 988 をリッスンし、ポート 988 または設定されたポートとの接続が自動的に許可されます。SMTPS プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に SMTPS プロトコルが開始され、認証が行われます。SMTPS は、電子メール送信用のプロトコルです。

電子メール プロキシの設定

要件

- 電子メール プロキシを経由してローカルとリモートの両方から電子メールにアクセスするユーザは、電子メール プログラムで、ローカル アクセス用とリモート アクセス用に別々の電子メール アカウントが必要です。
- 電子メール プロキシ セッションでユーザが認証される必要があります。

AAA サーバ グループの設定

ステップ 1　[Configuration] > [Features] > [VPN] > [E-mail Proxy] > [AAA] を参照します。

ステップ 2　該当のタブ（[POP3S]、[IMAP4S]、または [SMTPS]）を選択して、AAA サーバ グループを関連付け、これらのセッションに適用するデフォルトのグループ ポリシーを設定します。

- [AAA server groups]：[AAA Server Groups] パネル（[Configuration] > [Features] > [Properties] > [AAA Setup] > [AAA Server Groups]）に移動する場合にクリックします。ここでは、AAA サーバ グループを追加または編集できます。
- [group policies]：[Group Policy] パネル（[Configuration] > [Features] > [VPN] > [General] > [Group Policy]）に移動する場合にクリックします。ここでは、グループ ポリシーを追加または編集できます。
- [Authentication Server Group]：ユーザ認証用の認証サーバ グループを選択します。デフォルトでは、認証サーバが設定されていません。AAA を認証方式として設定した場合には（[Configuration] > [Features AAA] > [VPN] > [E-Mail Proxy] > [Authentication] パネル）、AAA サーバを設定してここで選択しないと、常に認証に失敗します。
- [Authorization Server Group]：ユーザ認可用の認可サーバ グループを選択します。デフォルトでは、認可サーバが設定されていません。
- [Accounting Server Group]：ユーザ アカウンティング用のアカウンティング サーバ グループを選択します。デフォルトでは、アカウンティング サーバが設定されていません。
- [Default Group Policy]：AAA が CLASSID 属性を返さない場合にユーザに適用するグループ ポリシーを選択します。長さは、4 ～ 15 文字の英数字です。デフォルトのグループ ポリシーを指定しなかった場合と、CLASSID が存在しない場合には、ASA がセッションを確立できません。
- [Authorization Settings]：ASA が認可のために認識するユーザ名の値を設定します。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 認可を必要とするユーザに適用されます。
  - [Use the entire DN as the username]：認可用の認定者名を使用する場合に選択します。
  - [Specify individual DN fields as the username]：ユーザ認可用に特定の DN フィールドを指定する場合に選択します。

    [DN] フィールドは、プライマリとセカンダリの 2 つを選択できます。たとえば、EA を選択した場合には、ユーザは電子メール アドレスによって認証されます。John Doe という一般名（CN）と johndoe@cisco.com という電子メール アドレスを持つユーザは、John Doe または johndoe として認証されません。彼は johndoe@cisco.com として認証される必要があります。EA および O を選択した場合、John Doe は johndoe@cisco.com および Cisco Systems, Inc. として認証される必要があります。
  - [Primary DN Field]：認可用に設定するプライマリ DN フィールドを選択します。デフォルト値は CN です。オプションには、次のものが含まれます。

DN フィールド	定義
Country（C）	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	ユーザ、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。

DN フィールド	定義
E-mail Address（EA）	証明書を所有するユーザ、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、または III などの世代修飾子。
Given Name（GN）	証明書所有者の名前（名）。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市町村。
Name（N）	証明書所有者の名前。
Organization（O）	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	証明書所有者の役職（Dr. など）。
User ID（UID）	証明書所有者の ID 番号。

  - [Secondary DN Field]：（オプション）認可用に設定するセカンダリ DN フィールドを選択します。デフォルト値は OU です。オプションには、上記の表に記載されているものすべてに加えて、[None] があります。これは、セカンダリ フィールドを指定しない場合に選択します。

電子メール プロキシを使用するインターフェイスの識別

[Email Proxy Access] 画面では、電子メール プロキシを設定するインターフェイスを識別できます。電子メール プロキシは、個々のインターフェイスで設定および編集できます。また、1 つのインターフェイスで電子メール プロキシを設定および編集すれば、その設定をすべてのインターフェイスに適用できます。管理専用のインターフェイスやサブインターフェイスに対して電子メール プロキシは設定できません。

ステップ 1　[Configuration] > [VPN] > [E-Mail Proxy] > [Access] を参照して、インターフェイスでイネーブルになっている電子メール プロキシを示します。

- [Interface]：設定されているすべてのインターフェイスの名前を表示します。
- [POP3S Enabled]：そのインターフェイスで POP3S がイネーブルかどうかを示します。
- [IMAP4s Enabled]：そのインターフェイスで IMAP4S がイネーブルかどうかを示します。
- [SMTPS Enabled]：そのインターフェイスで SMTPS がイネーブルかどうかを示します。

ステップ 2　強調表示されているインターフェイスの電子メール プロキシ設定を変更するには、[Edit] をクリックします。

電子メール プロキシの認証の設定

電子メール プロキシのタイプごとに認証方式を設定します。

ステップ 1　[Configuration] > [Features] > [VPN] > [E-mail Proxy] > [Authentication] を参照します。

ステップ 2　複数の認証方式から選択できます。

- [AAA]：AAA 認証を必須にする場合に選択します。このオプションを使用するには、AAA サーバを設定する必要があります。ユーザは、ユーザ名、サーバ、およびパスワードを入力します。ユーザは、VPN ユーザ名と電子メール ユーザ名の両方を入力する必要があります。そのとき、互いのユーザ名が異なる場合にだけ、VPN 名デリミタによって区切ります。
- [Certificate]：証明書認証を必須にする場合に選択します。
- 現在の ASA ソフトウェア リリースでは、電子メール プロキシに対して証明書認証が機能しません[Piggyback HTTPS]：ピギーバック認証を必須にする場合に選択します。

  この認証スキームは、ユーザがすでにクライアントレス SSL VPN セッションを確立していることを必須とします。ユーザは電子メール ユーザ名だけを入力します。パスワードは不要です。ユーザは、VPN ユーザ名と電子メール ユーザ名の両方を入力する必要があります。そのとき、互いのユーザ名が異なる場合にだけ、VPN 名デリミタによって区切ります。

  SMTPS 電子メールは、最も頻繁にピギーバックを使用します。ほとんどの SMTP サーバが、ユーザがログインすることを許可していないためです。

（注）　IMAP は、同時ユーザ数によって制限されない多数のセッションを生成しますが、ユーザ名に対して許可されている同時ログインの数を数えます。IMAP セッションの数がこの最大値を超え、クライアントレス SSL VPN 接続の有効期限が切れた場合には、その後ユーザが新しい接続を確立できません。以下の解決策があります。

- ユーザが IMAP アプリケーションを終了して ASA とのセッションをクリアしてから、新しいクライアントレス SSL VPN 接続を確立する。
- 管理者が IMAP ユーザの同時ログイン数を増やす（[Configuration] > [Features] > [VPN] > [General] > [Group Policy] > [Edit Group Policy] > [General]）。
- 電子メール プロキシの HTTPS/ピギーバック認証をディセーブルにする。

- [Mailhost]：（SMTPS のみ）メールホスト認証を必須にする場合に選択します。POP3S と IMAP4S は必ずメールホスト認証を実行するため、このオプションは、SMTPS の場合にだけ表示されます。この認証方式では、ユーザの電子メール ユーザ名、サーバ、およびパスワードが必要です。

プロキシ サーバの識別

この [Default Server] パネルでは、ASA のプロキシ サーバを識別し、電子メール プロキシのデフォルト サーバ、ポート、および非認証セッション制限を設定することができます。

ステップ 1　[Configuration] > [Features] > [VPN] > [E-mail Proxy] > [Default Servers] を参照します。

ステップ 2　次のフィールドを設定します。

- [Name or IP Address]：デフォルトの電子メール プロキシ サーバの DNS 名または IP アドレスを入力します。
- [Port]：ASA が電子メール プロキシ トラフィックをリッスンするポート番号を入力します。設定されたポートに対する接続が自動的に許可されます。電子メール プロキシは、SSL 接続だけをこのポートで許可します。SSL トンネルが確立された後に電子メール プロキシが開始され、認証が行われます。

  デフォルトの設定は次のとおりです。

  - 995（POP3 の場合）
  - 993（IMAP4S の場合）
  - 988（SMTPS の場合）
- [Enable non-authenticated session limit]：非認証電子メール プロキシ セッションの数を制限する場合に選択します。認証プロセスでのセッションの制限を設定でき、それによって DOS 攻撃を防ぎます。新しいセッションが、設定された制限を超えると、ASA が最も古い非認証接続を終了します。非認証接続が存在しない場合には、最も古い認証接続が終了します。それによって認証済みのセッションが終了することはありません。

  電子メール プロキシ接続には、3 つの状態があります。

  1. 新規に電子メール接続が確立されると、「認証されていない」状態になります。
  2. この接続でユーザ名が提示されると、「認証中」状態になります。
  3. ASA が接続を認証すると、「認証済み」状態になります。

デリミタの設定

このパネルでは、電子メール プロキシ認証で使用するユーザ名/パスワード デリミタとサーバ デリミタを設定します。

ステップ 1　[Configuration] > [Features] > [VPN] > [E-mail Proxy] > [Delimiters] を参照します。

ステップ 2　次のフィールドを設定します。

- [Username/Password Delimiter]：VPN ユーザ名と電子メール ユーザ名を区切るためのデリミタを選択します。電子メール プロキシで AAA 認証を使用する場合、および VPN ユーザ名と電子メール ユーザ名が異なる場合に両方のユーザ名を使用します。電子メール プロキシ セッションにログインするときに、ユーザは両方のユーザ名を入力し、ここで設定したデリミタで区切ります。また、電子メール サーバ名も入力します。

（注）　クライアントレス SSL VPN 電子メール プロキシ ユーザのパスワードに、デリミタとして使用されている文字を含めることはできません。

- [Server Delimiter]：ユーザ名と電子メール サーバ名を区切るためのデリミタを選択します。このデリミタは、VPN 名デリミタとは別にする必要があります。電子メール プロキシ セッションにログインする場合には、ユーザ名フィールドにユーザ名とサーバの両方を入力します。

  たとえば、VPN 名デリミタとして : を使用し、サーバ デリミタとして @ を使用する場合には、電子メール プロキシ経由で電子メール プログラムにログインするときに、vpn_username:e-mail_username@server という形式でユーザ名を入力します。

VPN の監視

VPN 接続グラフの監視

ASA の VPN 接続データをグラフ形式または表形式で表示するには、次の画面を参照してください。

[Monitor IPsec Tunnels]：[Monitoring] > [VPN] > [VPN Connection Graphs] > [IPSec Tunnels]

表示や、エクスポートまたは印刷の準備を行う IPsec トンネル タイプのグラフとテーブルを指定します。

[Monitor L2TP]：[Monitoring] > [Features] > [VPN] > [VPN Connection Graphs] > [L2TP]

表示するグラフまたはテーブルのタイプを指定します。

[Monitor Sessions]：[Monitoring] > [VPN] > [VPN Connection Graphs] > [Sessions]

表示や、エクスポートまたは印刷の準備を行う VPN セッション タイプのグラフとテーブルを指定します。

VPN 統計の監視

特定のリモート アクセス、LAN 間、クライアントレス SSL VPN、または電子メール プロキシ セッションの詳細なパラメータおよび統計情報を表示するには、次の画面を参照してください。パラメータと統計情報は、セッション プロトコルによって異なります。また、統計情報テーブルの内容は、選択した接続のタイプによって異なります。各詳細テーブルには、それぞれのセッションの関連パラメータがすべて表示されます。

[Monitor Session] ウィンドウ：[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]

ASA の VPN セッション統計情報を表示します。このペインの 2 番目のテーブルの内容は、[Filter By] リストの選択によって異なります。

（注）　管理者は、非アクティブ状態のユーザ数をトレースし、統計情報を確認できるようになりました。ライセンス キャパシティに到達せず、新規ユーザがログインできるように、最長時間非アクティブなセッションはアイドルとマークされます（さらに自動的にログオフされます）。これらの統計情報には、**show vpn-sessiondb** CLI コマンド（『Cisco Security Appliance Command Reference Guide』を参照）を使用してアクセスすることもできます。

- [All Remote Access]

このテーブルの値がリモート アクセス（IPsec ソフトウェアおよびハードウェア クライアント）トラフィックに関連することを示します。

- [Username/Connection Profile]：セッションのユーザ名またはログイン名、および接続プロファイル（トンネル グループ）を示します。クライアントが認証にデジタル証明書を使用している場合、フィールドに証明書の Subject CN または Subject OU が表示されます。
- [Group Policy Connection Profile]：セッションのトンネル グループ ポリシー接続プロファイルが表示されます。
- [Assigned IP Address/Public IP Address]：このセッションのリモート クライアントに割り当てられているプライベート（「割り当てられた」）IP アドレスを示します。これは「内部」または「仮想」IP アドレスとも呼ばれ、クライアントはプライベート ネットワーク上のホストとして表示されます。また、このリモート アクセス セッションのクライアントのパブリック IP アドレスも表示します。パブリック IP アドレスは、「外部」IP アドレスとも呼ばれます。通常、これは ISP によってクライアントに割り当てられます。このアドレスにより、クライアントは、パブリック ネットワーク上のホストとして機能することが可能となります。

  （注）　[Assigned IP Address] フィールドは、クライアントレス SSL VPN セッションには適用されません。ASA（プロキシ）がすべてのトラフィックの送信元になります。ネットワーク拡張モードにおけるハードウェア クライアント セッションの場合、割り当てられた IP アドレスは、ハードウェア クライアントのプライベート/内部ネットワーク インターフェイスのサブネットです。

- [Ping]：ネットワークの接続テストのために、ICMP `ping`（Packet Internet Groper）パケットを送信します。具体的には、ASA は、選択したホストに ICMP Echo Request メッセージを送信します。ホストが到達可能な場合、Echo Reply メッセージを返し、ASA はテストしたホストの名前が記された Success メッセージ、および要求を送信して応答を受信するまでの経過時間を表示します。何らかの理由でシステムが到達不可能な場合（ホストがダウンしている、ICMP がホストで実行していない、ルートが設定されていない、中間ルータがダウンしている、ネットワークがダウンまたは輻輳しているなど）、ASA には、テストしたホストの名前が記された [Error] 画面が表示されます。
- [Logout By]：ログアウトするセッションのフィルタリングに使う基準を選択します。--All Sessions-- 以外を選択した場合、[Logout By] リストの右側のボックスがアクティブになります。値に Protocol for Logout By を選択した場合、ボックスがリストに変わり、ログアウト フィルタとして使用するプロトコル タイプを選択できます。このリストのデフォルト値は IPsec です。Protocol 以外の値を選択した場合は、このボックスに適切な値を入力する必要があります。

[Monitor Active AnyConnect Sessions]：[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]

ユーザ名、IP アドレス、アドレス タイプ、またはパブリック アドレスでソートされた AnyConnect クライアント セッションを表示します。

[Monitor VPN Session Details]：[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] > [Details]

選択したセッションのコンフィギュレーション設定、統計情報、およびステート情報を表示します。

- [NAC Result and Posture Token]

ASDM では、ASA でネットワーク アドミッション コントロールを設定している場合にだけ、このカラムに値が表示されます。

  - [Accepted]：ACS は正常にリモート ホストのポスチャを検証しました。
  - [Rejected]：ACS はリモート ホストのポスチャの検証に失敗しました。
  - [Exempted]：ASA に設定されたポスチャ検証免除リストに従って、リモート ホストはポスチャ検証を免除されました。
  - [Non-Responsive]：リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。
  - [Hold-off]：ポスチャ検証に成功した後、ASA とリモート ホストの EAPoUDP 通信が途絶えました。
  - [N/A] : VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。
  - [Unknown]：ポスチャ検証が進行中です。

  ポスチャ トークンは、Access Control Server で設定可能な情報文字列です。ACS は情報提供のために ASA にポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。NAC Result に続く一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected または Unknown です。

  [Session Details] ペインの [Details] タブには、次のカラムが表示されます。

  - [ID]：セッションにダイナミックに割り当てられた一意の ID。ID は、セッションへの ASA のインデックスとして機能します。このインデックスを使用して、セッションに関する情報を維持および表示します。
  - [Type]：セッションのタイプ。IKE、IPsec または NAC。
  - [Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol, and Port]：実際の（ローカル）ピアの両方に割り当てられているアドレスとポートと外部ルーティングのためにそのピアに割り当てられているアドレスとポート。
  - [Encryption]：このセッションで使用しているデータ暗号化アルゴリズム（ある場合）。
  - [Assigned IP Address and Public IP Address]：このセッションのリモート ピアに割り当てられているプライベート IP アドレスを示します。内部または仮想 IP アドレスとも呼ばれ、割り当てられている IP アドレスによって、リモート ピアはプライベート ネットワーク上にあるように見えます。2 番目のフィールドには、このセッションのリモート コンピュータのパブリック IP アドレスが表示されます。外部 IP アドレスとも呼ばれ、通常、パブリック IP アドレスは ISP によってリモート コンピュータに割り当てられます。これによって、リモート コンピュータはパブリック ネットワークのホストとして機能できます。
  - [Other]：セッションに関連付けられているその他の属性。

次の属性は、IKE セッション、IPsec セッション、および NAC セッションに適用されます。

- [Revalidation Time Interval]：成功した各ポスチャ検証間に必要とされる間隔（秒数）。
- [Time Until Next Revalidation]：最後のポスチャ検証試行が成功しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
- [Status Query Time Interval]：成功したポスチャ検証またはステータス クエリーの応答と次のステータス クエリーの応答との間に許容される時間（秒数）。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、ASA がリモート ホストに発行する要求です。
- [EAPoUDP Session Age]：最後に成功したポスチャ検証から経過した秒数。
- [Hold-Off Time Remaining]：最後のポスチャ検証が成功した場合は 0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
- [Posture Token]：Access Control Server で設定可能な情報文字列。ACS は情報提供のために ASA にポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
- [Redirect URL]：ポスチャ検証またはクライアントなしの認証が終わると、ACS はセッション用のアクセス ポリシーを ASA にダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。ASA は、リモート ホストのすべての HTTP（ポート 80）要求および HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセス ポリシーに Redirect URL が含まれていない場合、ASA はリモート ホストからの HTTP 要求および HTTPS 要求をリダイレクトしません。

  Redirect URL は、IPsec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。

  [More]：このボタンを押して、セッションやトンネル グループを再検証または初期化します。

ACL タブには、セッションに一致した ACE が含まれる ACL が表示されます。

[Monitor Cluster Loads]：[Monitoring] > [VPN] > [VPN Statistics] > [Cluster Loads]

VPN ロードバランシング クラスタ内のサーバ間における現在のトラフィックの負荷分散を表示します。サーバがクラスタの一部でない場合、このサーバが VPN ロードバランシング クラスタに参加していない旨を伝える情報メッセージが表示されます。

[Monitor Crypto Statistics]：[Monitoring] > [VPN] > [VPN Statistics] > [Crypto Statistics]

ASA で現在アクティブなユーザおよび管理者セッションの暗号統計情報を表示します。テーブルの各行は、1 つの暗号統計情報を表します。

[Monitor Compression Statistics]：[Monitoring] > [VPN] > [VPN Statistics] > [Compression Statistics]

ASA で現在アクティブなユーザおよび管理者セッションの圧縮統計情報を表示します。テーブルの各行は、1 つの圧縮統計情報を表します。

[Monitor Encryption Statistics]：[Monitoring] > [VPN] > [VPN Statistics] > [Encryption Statistics]

ASA で現在アクティブなユーザおよび管理者セッションによって使用されるデータ暗号化アルゴリズムを表示します。テーブルの各行は、1 つの暗号化アルゴリズム タイプを表します。

[Monitor Global IKE/IPsec Statistics]：[Monitoring] > [VPN] > [VPN Statistics] > [Global IKE/IPSec Statistics]

ASA で現在アクティブなユーザおよび管理者セッションのグローバル IKE/IPsec 統計情報を表示します。テーブルの各行は、1 つのグローバル統計情報を表します。

[Monitor NAC Session Summary]

アクティブな累積ネットワーク アドミッション コントロール セッションを表示します。

- [Active NAC Sessions]：ポスチャ検証の対象のリモート ピアに関する一般的な統計情報。
- [Cumulative NAC Sessions]：現在ポスチャ検証の対象か、または以前から対象だったリモート ピアに関する一般的な統計情報。
- [Accepted]：ポスチャ検証に成功し、Access Control Server によってアクセス ポリシーが与えられたピアの数。
- [Rejected]：ポスチャ検証に失敗し、Access Control Server によってアクセス ポリシーが与えられなかったピアの数。
- [Exempted]：ASA で設定された [Posture Validation Exception] リストのエントリに一致するため、ポスチャ検証の対象になっていないピアの数。
- [Non-responsive]：Extensible Authentication Protocol（EAP）over UDP のポスチャ検証要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。ASA のコンフィギュレーションがクライアントレス ホストをサポートする場合、Access Control Server は、クライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアの ASA にダウンロードします。クライアントレス ホストをサポートしない場合、ASA は NAC デフォルト ポリシーを割り当てます。
- [Hold-off]：ポスチャ検証が成功した後に、ASA が EAPoUDP 通信を失ったピアの数。NAC Hold Timer 属性（[Configuration] > [VPN] > [NAC]）は、このタイプのイベントと次のポスチャ検証試行との間の遅延時間を判定します。
- [N/A]：VPN NAC グループ ポリシーに従って NAC が無効になっているピアの数。
- [Revalidate All]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）が変更された場合にクリックします。このボタンをクリックすると、ASA によって管理されるすべての NAC セッションの新しい無条件のポスチャ検証を開始します。このボタンをクリックするまで各セッションに対して有効だったポスチャ検証と割り当てられているアクセス ポリシーは、新しいポスチャ検証が成功または失敗するまで有効のままとなります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。
- [Initialize All]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）が変更され、セッションに割り当てられているリソースをクリアする場合にクリックします。このボタンをクリックすると、ASA によって管理されるすべての NAC セッションのポスチャ検証で使用される EAPoUDP アソシエーションと割り当てられているアクセス ポリシーをパージし、新しい無条件のポスチャ検証を開始します。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザ トラフィックに影響する場合があります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。

[Monitor Protocol Statistics]：[Monitoring] > [VPN] > [VPN Statistics] > [Protocol Statistics]

ASA で現在アクティブなユーザおよび管理者セッションによって使用されるプロトコルを表示します。テーブルの各行は、1 つのプロトコル タイプを表します。

[Monitor VLAN Mapping Sessions]

使用中の各グループ ポリシーの Restrict Access to VLAN パラメータの値で判別された、出力 VLAN に割り当てられているセッション数を表示します。ASA はすべてのトラフィックを指定された VLAN に転送します。

[Monitor SSO Statistics for Clientless SSL VPN Session]：[Monitoring] > [VPN] > [WebVPN] > [SSO Statistics]

ASA に設定されている現在アクティブなシングル サインオン（SSO）サーバの SSO 統計情報を表示します。

（注）　これらの統計情報は、SiteMinder サーバおよび SAML Browser Post Profile サーバの SSO に関するものだけです。

CHAPTER 8

SSL 設定

SSL 設定

[Configuration] > [Device Management] > [Advanced] > [SSL Settings]

[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]

ASA は、Secure Sockets Layer（SSL）プロトコルおよび Transport Layer Security（TLS）を使用して、ASDM、クライアントレス SSL VPN、VPN、およびブラウザベースのセッションのセキュアなメッセージ伝送を実現します。[SSL Settings] ペインでは、クライアントとサーバの SSL バージョンおよび暗号化アルゴリズムを設定できます。また、以前に設定したトラストポイントを特定のインターフェイスに適用したり、関連付けられたトラストポイントのないインターフェイスのフォールバック トラストポイントを設定したりすることもできます。

（注） リリース 9.3（2）では、SSLv3 は廃止されています。現在のデフォルトは [any] ではなく [tlsv1] です。[any] キーワードは廃止されました。[any]、[sslv3] または [sslv3-only] を選択した場合、設定は受け入れられますが警告が表示されます。[OK] をクリックして作業を続行します。ASA の次のメジャー リリースでは、これらのキーワードは ASA から削除されます。

フィールド

- [Server SSL Version]：サーバとして動作するときに ASA が使用する最小の SSL/TLS プロトコル バージョンをドロップダウン リストから指定します。

Any	SSLv2 クライアントの hello を受け入れ、共通の最新バージョンをネゴシエートします。
SSL V3	SSLv2 クライアントの hello を受け入れ、SSLv3（以降）をネゴシエートします。
TLS V1	SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートします。
TLSV1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートします。

- [Client SSL Version]：クライアントとして動作するときに ASA が使用する最小の SSL/TLS プロトコル バージョンをドロップダウン リストから指定します。

Any	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
SSL V3	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
TLS V1	TLSv1 クライアントの hello を送信し、TLSv1（以降）をネゴシエートします。
TLSV1.1	TLSv1.1 クライアントの hello を送信し、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	TLSv1.2 クライアントの hello を送信し、TLSv1.2（以降）をネゴシエートします。

- [Diffie-Hellmann group to be used with SSL]：ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group1]（768 ビット絶対値）、[Group2]（1024 ビット絶対値）、[Group5]（1536 ビット絶対値）、[Group14]（2048 ビット絶対値、224 ビット素数位数）、および [Group24]（2048 ビット絶対値、256 ビット素数位数）です。デフォルト値は [Group2] です。
- SSL 暗号化アルゴリズムを指定します。[Configure Cipher Algorithms/Custom String] ダイアログボックスを使用してテーブル エントリを定義または変更するには、[Edit] をクリックします。SSL 暗号のセキュリティ レベルを選択し、[OK] をクリックします。
  - [Cipher Version]：ASA でサポートされ、SSL 接続に使用される暗号バージョンを一覧表示します。
  - [Cipher Security Level]：ASA でサポートされ、SSL 接続に使用される暗号セキュリティ レベルを一覧表示します。次のいずれかのオプションを選択します。

    [All]：NULL-SHA を含むすべての暗号。

    [Low]：NULL-SHA を除くすべての暗号。

    [Medium]：NULL-SHA、DES-CBC-SHA、RC4-SHA、および RC4-MD5 を除くすべての暗号（これがデフォルトです）。

    [Fips]：NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く FIPS 準拠のすべての暗号。

    [High]：SHA-2 を使用する AES-256 暗号だけが含まれ、TLS バージョン 1.2 にのみ適用されます。

    [Custom]：[Cipher algorithms/custom string] ボックスで指定する 1 つ以上の暗号。このオプションでは、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。
  - [Cipher Algorithms/Custom String]：ASA でサポートされ、SSL 接続に使用される暗号アルゴリズムを一覧表示します。OpenSSL を使用した暗号の詳細については、https://www.openssl.org/docs/apps/ciphers.html を参照してください。

    ASA では、サポートされる暗号の優先順位が次のように指定されています。

    TLSv1.2 だけでサポートされる暗号

DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256
DHE-RSA-AES256-SHA
AES256-SHA
DHE-RSA-AES128-SHA
AES128-SHA
DES-CBC3-SHA

TLSv1.1 または TLSv1.2 でサポートされない暗号

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

- [Server Name Indication (SNI)]：ドメイン名とそのドメインに関連付けるトラストポイントを指定します。[Add/Edit Server Name Indication (SNI)] ダイアログボックスを使用して各インターフェイスのドメインおよびトラストポイントを定義または変更するには、[Add] または [Edit] をクリックします。
  - [Specify domain]：ドメイン名を入力します。
  - [Select trustpoint to associate with domain]：ドロップダウン リストからトラストポイントを選択します。
- [Certificates]：各インターフェイスの SSL 認証に使用する証明書を割り当てます。[Select SSL Certificate] ダイアログボックスを使用して各インターフェイスのトラストポイントを定義または変更するには、[Edit] をクリックします。
  - [Primary Enrolled Certificate]：このインターフェイスの証明書に使用するトラストポイントを選択します。
  - [Load Balancing Enrolled Certificate]：VPN ロード バランシングが設定されている場合、証明書で使用するトラストポイントを選択します。
- [Fallback Certificate]：証明書が関連付けられていないインターフェイスで使用する証明書を選択します。[None] を選択すると、ASA はデフォルトの RSA キー ペアと証明書を使用します。
- [Forced Certification Authentication Timeout]：証明書認証がタイムアウトするまでの分数を設定します。
- [Apply]：変更内容を保存します。
- [Reset]：変更内容を取り消し、SSL パラメータを以前に定義した値にリセットします。

CHAPTER 9

認可および認証用の外部サーバ

この章では、ASA で AAA をサポートするための外部 LDAP、RADIUS、または TACACS+ サーバの設定方法について説明します。外部サーバを使用するように ASA を設定する前に、正しい ASA 許可属性でサーバを設定し、それらの属性のサブセットから個々のユーザに対する個別の許可を割り当てる必要があります。

許可属性のポリシー実施の概要

ASA は、ユーザ認可属性（ユーザ権利またはユーザ権限とも呼ばれる）を VPN 接続に適用するためのいくつかの方法をサポートしています。ASA を設定して、次のいずれかの組み合わせからユーザ属性を取得できます。

- ASA のダイナミック アクセス ポリシー（DAP）
- 外部 RADIUS または LDAP 認証および許可サーバ（およびその両方）
- ASA のグループ ポリシー

ASA がすべてのソースから属性を受信すると、その属性が評価され、集約されてユーザ ポリシーに適用されます。属性の間で衝突がある場合、DAP 属性が優先されます。

ASA によって属性が適用される順序は次のとおりです（図 9-1 を参照）。

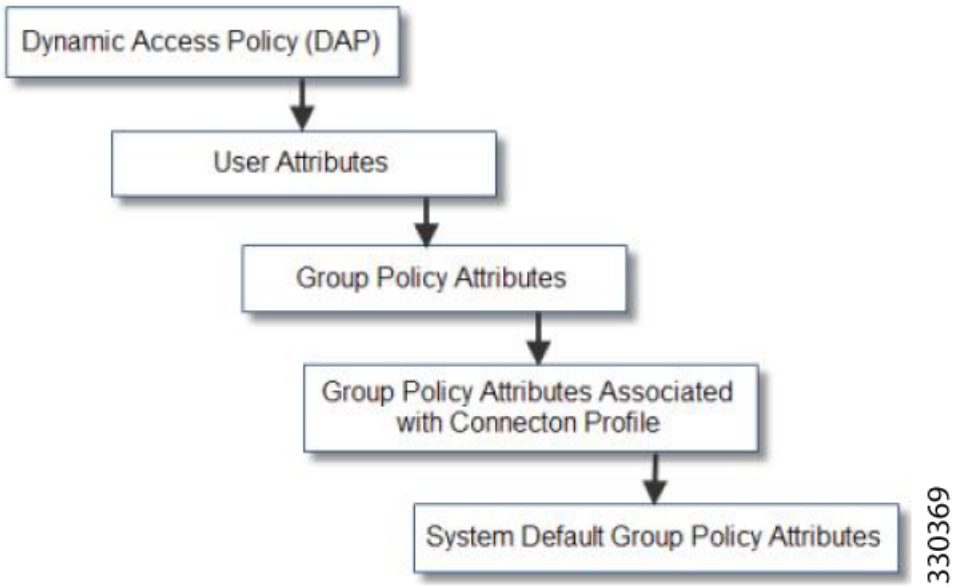
1. ASA 上の DAP 属性：バージョン 8.0(2) で導入されたこの属性は、他のすべての属性よりも優先されます。DAP 内でブックマークまたは URL リストを設定した場合は、グループ ポリシーで設定されているブックマークや URL リストよりも優先されます。
2. AAA サーバ上のユーザ属性：ユーザ認証や認可が成功すると、サーバからこの属性が返されます。これらの属性を、ASA のローカル AAA データベースの個々のユーザに設定されている属性（ASDM のユーザ アカウント）と混同しないでください。
3. ASA 上で設定されているグループ ポリシー：RADIUS サーバからユーザの RADIUS CLASS 属性 IETF-Class-25（OU=*group-policy*）の値が返された場合は、ASA はそのユーザを同じ名前のグループ ポリシーに入れて、そのグループ ポリシーの属性のうち、サーバから返されないものを適用します。

   LDAP サーバでは、任意の属性名を使用してセッションのグループ ポリシーを設定できます。ASA 上で設定されている LDAP 属性マップによって、LDAP 属性が Cisco 属性 IETF-Radius-Class にマッピングされます。

4. 接続プロファイル（CLI では「トンネル グループ」と呼ばれます）によって割り当てられたグループ ポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザに適用されるデフォルトのグループ ポリシーが含まれています。ASA に接続するすべてのユーザは、最初にこのグループに所属します。このグループでは、DAP、サーバから返されるユーザ属性、またはユーザに割り当てられたグループ ポリシーにはない属性が定義されています。
5. ASA で割り当てられたデフォルトのグループ ポリシー（DfltGrpPolicy）：システムのデフォルト属性は、DAP、ユーザ属性、グループ ポリシー、または接続プロファイルで不足している値を提供します。

ASA LDAP コンフィギュレーションの定義

図 9-1　　ポリシー実施フロー



認可では、権限または属性を使用するプロセスを参照します。認証または認可サーバとして定義されている LDAP サーバは、権限または属性（設定されている場合）を適用します。

ガイドライン

ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を使用します。RADIUS 属性は、名前ではなく数値 ID によって適用されます。

ASDM バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。ASDM バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 属性は、RADIUS の章に記載されている RADIUS 属性のサブセットです。

Active Directory/LDAP VPN リモート アクセス認可の例

この項では、Microsoft Active Directory サーバを使用している ASA で認証および認可を設定するための手順の例を示します。説明する項目は次のとおりです。

その他の設定例については、Cisco.com にある次のテクニカル ノートを参照してください。

- 『*ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example*』
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml
- 『*PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login*』
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808d1a7c.shtml

ユーザベースの属性ポリシーの適用

すべての標準 LDAP 属性は、予約済みのベンダー固有属性（VSA）にマッピングできます。また、1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングできます。

次の例では、AD の LDAP サーバで設定されたユーザに対し、簡単なバナーを適用するように ASA を設定します。サーバ上で [General] タブの [Office] フィールドを使用してバナー テキストを入力します。このフィールドでは、physicalDeliveryOfficeName という名前の属性を使用します。ASA で、physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングする属性マップを作成します。認証の間に、ASA はサーバから physicalDeliveryOfficeName の値を取得し、その値を Cisco 属性 Banner1 にマッピングしてユーザにバナーを表示します。

この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続を使用して接続します。

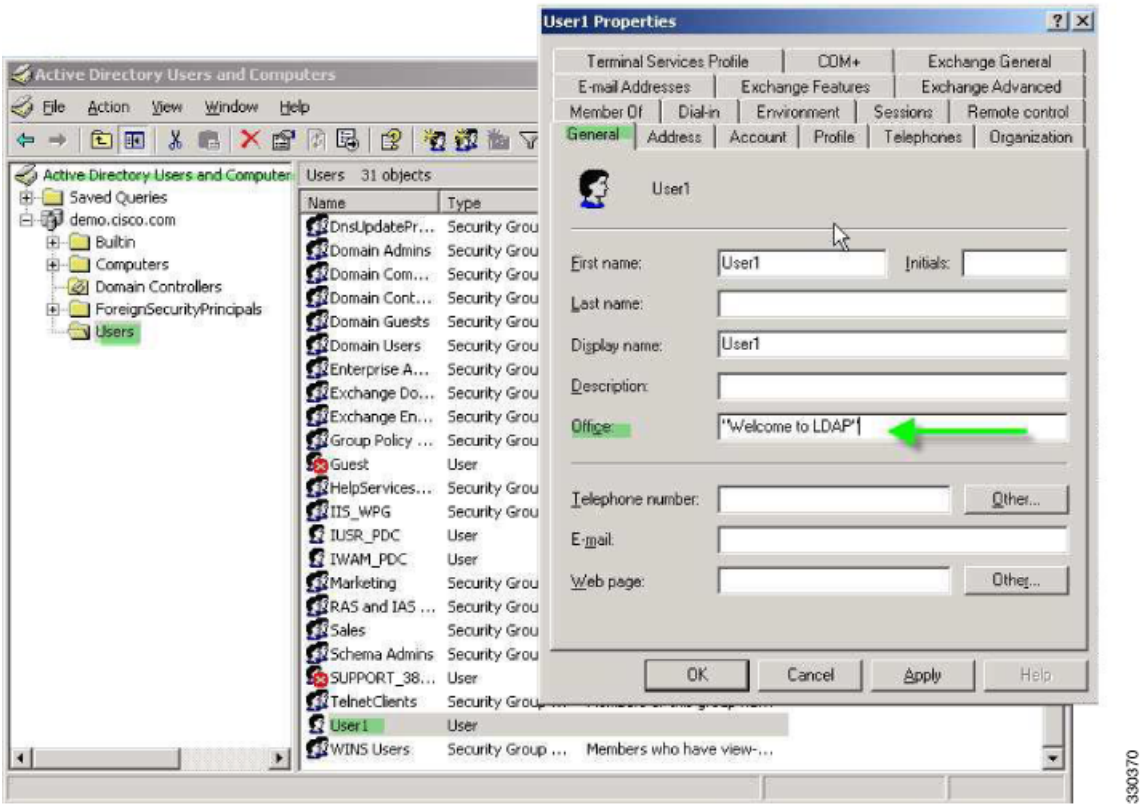
ユーザの属性を AD または LDAP サーバ上で設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます（図 9-2 を参照）。

ステップ 2　[General] タブをクリックし、バナー テキストを [Office] フィールドに入力します。このフィールドでは、AD/LDAP 属性 physicalDeliveryOfficeName が使用されます。

図 9-2　　LDAP ユーザの設定



ステップ 3　ASA 上で LDAP 属性マップを作成します。

次の例では、Banner というマップを作成し、AD/LDAP 属性 physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングします。

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

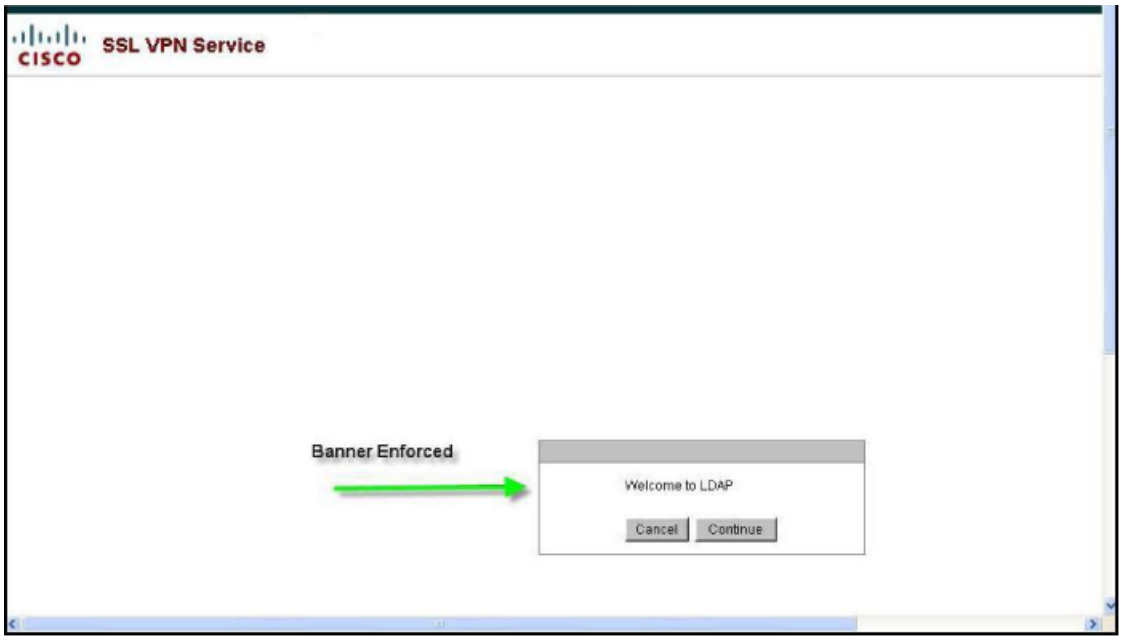
次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ Banner を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

ステップ 5　バナーの適用をテストします。

クライアントレス SSL 接続の例を次に示します。このバナーは、ユーザ認証後に属性マップ経由で適用されたものです（図 9-3 を参照）。

図 9-3　　表示されたバナー



特定のグループ ポリシーへの LDAP ユーザの配置

次に示す例では、AD LDAP サーバ上の User1 を ASA 上の特定のグループ ポリシーに対して認証する方法について説明します。サーバで、[Organization] タブの [Department] フィールドを使用して、グループ ポリシーの名前を入力します。次に、属性マップを作成し、[Department] を Cisco 属性である IETF-Radius-Class にマッピングします。認証の間に、ASA はサーバから [Department] の値を取得し、その値を IETF-Radius-Class にマッピングして User1 をグループ ポリシーに配置します。

この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続経由で接続します。

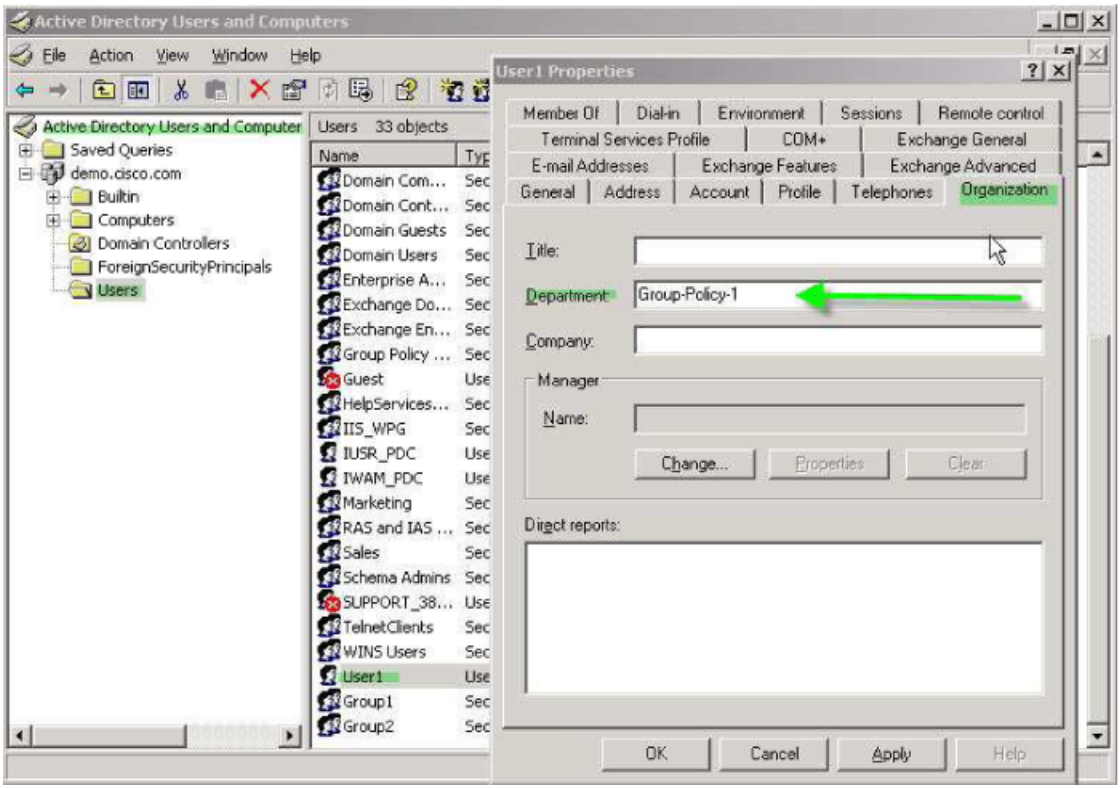
AD LDAP サーバ上のユーザの属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます（図 9-4 を参照）。

ステップ 2　[Organization] タブをクリックして、[Department] フィールドに **Group-Policy-1** と入力します。

図 9-4　AD/LDAP の [Department] 属性



ステップ 3　ステップ 1 に示した LDAP コンフィギュレーションの属性マップを定義します。

次の例では、AD 属性 Department を Cisco 属性 IETF-Radius-Class にマッピングする方法について説明します。

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ group_policy を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map group_policy
```

ステップ 5　ASA で新しいグループ ポリシーを追加し、ユーザに割り当てるために必要なポリシー属性を設定します。次の例では、Group-policy-1 を作成します。この名前は、サーバで [Department] フィールドに入力したものです。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

ステップ 6　このユーザとして VPN 接続を確立し、Group-Policy1 からの属性（およびその他に適用可能な、デフォルトのグループ ポリシーからの属性）がセッションに継承されていることを確認します。

ステップ 7　ASA とサーバの間の通信をモニタするには、特権 EXEC モードで **debug ldap 255** コマンドをイネーブルにします。このコマンドからの出力の例を次に示します。これは、主要なメッセージがわかるように編集済みです。

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

AnyConnect トンネルへのスタティック IP アドレスの割り当て

この例では、AnyConnect クライアント ユーザ Web1 を、特定のスタティック IP アドレスを受信するように設定します。そのアドレスを、AD LDAP サーバで [Dialin] タブの [Assign Static IP Address] フィールドに入力します。このフィールドでは、msRADIUSFramedIPAddress 属性を使用します。この属性を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする属性マップを作成します。

認証時に、ASA は msRADIUSFramedIPAddress の値をサーバから取得し、その値を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングし、スタティック アドレスを User1 に渡します。

次の例が当てはまるのは、フルトンネル クライアント、つまり IPsec クライアントや SSL VPN クライアント（AnyConnect クライアント 2.x および SSL VPN クライアント）などです。

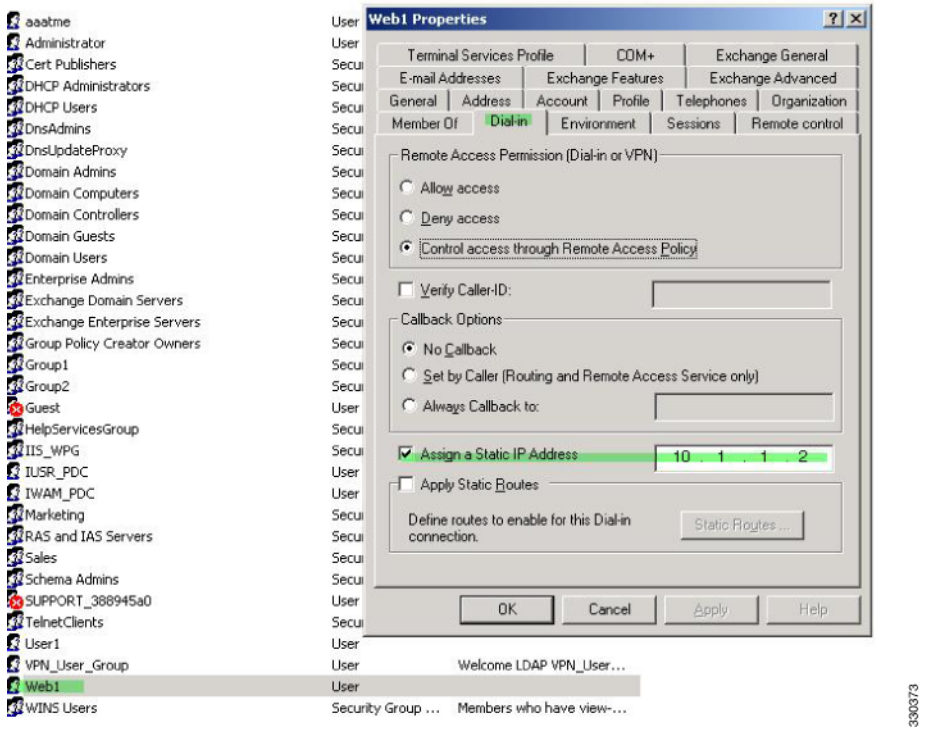
AD/LDAP サーバ上でユーザ属性を設定するには、次の手順を実行します。

ステップ 1　ユーザ名を右クリックします。

[Properties] ダイアログボックスが表示されます（図 9-5 を参照）。

ステップ 2　[Dialin] タブをクリックし、[Assign Static IP Address] チェックボックスをオンにして、IP アドレス 10.1.1.2 を入力します。

図 9-5　スタティック IP アドレスの割り当て



ステップ 3　ステップ 1 に示した LDAP コンフィギュレーションの属性マップを作成します。

次の例では、スタティック アドレス フィールドで使用されている AD 属性 msRADIUSFramedIPAddress を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする方法を示します。

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ static_address を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

ステップ 5　**vpn-address-assignment** コマンドが AAA を指定するように設定されているかどうかを確認するために、コンフィギュレーションのこの部分を **show run all vpn-addr-assign** コマンドで表示します。

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa    << これが設定されていることを確認します >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

ステップ 6　ASA と AnyConnect クライアントとの接続を確立します。次のことを確認します。

- バナーがクライアントレス接続と同じシーケンスで受信されている（図 9-6 を参照）。
- サーバ上で設定されて ASA にマッピングされた IP アドレスをユーザが受信している（図 9-7 を参照）。

図 9-6　AnyConnect セッションのバナーの確認

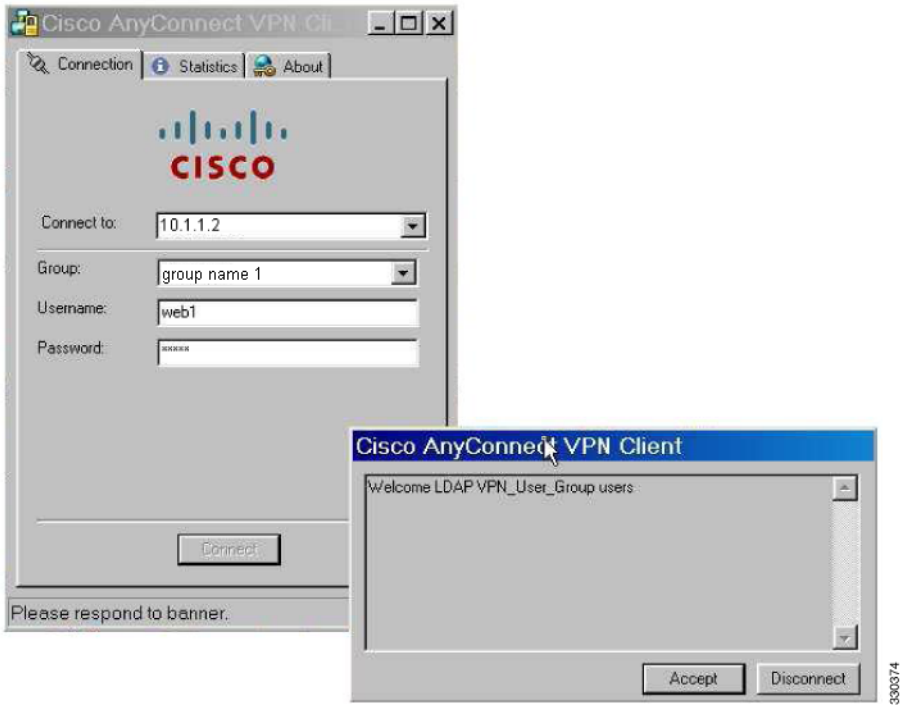


図 9-7　　確立された AnyConnect セッション

ステップ 7　**show vpn-sessiondb svc** コマンドを使用してセッションの詳細を表示し、割り当てられたアドレスを確認します。

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

ダイヤルインの許可または拒否アクセスの適用

次の例では LDAP 属性マップを作成し、ユーザによって許可されるトンネリング プロトコルを指定します。[Dialin] タブでの許可アクセスと拒否アクセスの設定を、Cisco 属性 Tunneling-Protocol にマッピングします。この属性では、表 9-1 に示すビットマップ値がサポートされます。

表 9-1　　Cisco Tunneling-Protocol 属性のビットマップ値

値	トンネリング プロトコル
1	PPTP
2	L2TP
4[1]	IPsec（IKEv1）
8[2]	L2TP/IPsec

表 9-1　Cisco Tunneling-Protocol 属性のビットマップ値 （続き）

値	トンネリング プロトコル
16	クライアントレス SSL
32	SSL クライアント：AnyConnect または SSL VPN クライアント
64	IPsec（IKEv2）

1. IPsec と L2TP over IPsec は同時にはサポートされません。そのため、値 4 と 8 は相互排他値となります。
2. 注 1 を参照してください。

この属性を使用して、プロトコルの [Allow Access]（TRUE）または [Deny Access]（FALSE）の条件を作成し、ユーザがアクセスを許可される方法を適用します。

この単純化した例では、トンネル プロトコル IPsec/IKEv1（4）をマッピングすることによって、Cisco VPN クライアントの許可（true）条件を作成できます。また、WebVPN（16）と SVC/AC（32）を値 48（16+32）としてマッピングし、拒否（false）条件を作成します。これで、ユーザは ASA に IPsec を使用して接続できるようになりますが、クライアントレス SSL または AnyConnect クライアントを使用して接続しようとすると拒否されます。

ダイヤルイン許可アクセスまたは拒否アクセスを適用する別の例については、次の URL にあるテクニカル ノート『*ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example*』を参照してください。

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml

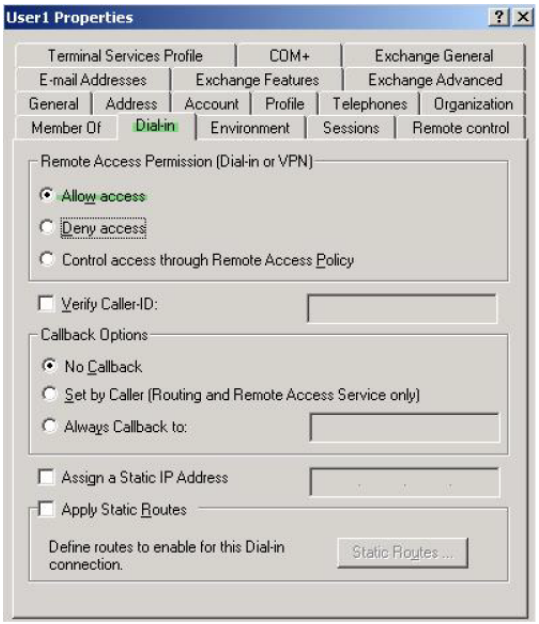
AD/LDAP サーバ上のユーザに属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます。

ステップ 2　[Dial-in] タブをクリックしてから、[Allow Access] オプション ボタンをクリックします（図 9-8）。

図 9-8　AD/LDAP User1 - [Allow Access]



（注）　[Control access through the Remote Access Policy] オプションを選択した場合は、値はサーバから返されず、適用される権限は ASA の内部グループ ポリシー設定に基づいて決定されます。

ステップ 3　IPsec と AnyConnect の両方の接続を許可するがクライアントレス SSL 接続を拒否する属性マップを作成します。

この例では、初めに tunneling_protocols というマップを作成します。次に、[Allow Access] 設定で使用される AD 属性 msNPAllowDialin を、**map-name** コマンドを使用して Cisco 属性 Tunneling-Protocols にマッピングします。次に、マップ値を **map-value** コマンドで追加します。

```
hostname(config)# ldap attribute-map tunneling_protocols
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 2 で作成した属性マップ tunneling_protocols を関連付けます。

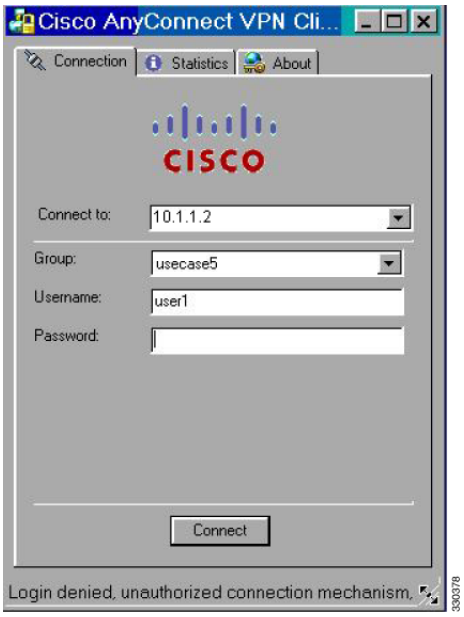
```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

ステップ 5　属性マップが設定したとおりに機能することを確認します。

ステップ 6　クライアントレス SSL、AnyConnect クライアント、および IPsec クライアントを使用して接続を試みます。クライアントレス SSL と AnyConnect では接続に失敗し、その原因が認可されていない接続メカニズムにあることを示すメッセージが表示されます。IPsec クライアントの接続は成功します。IPsec は、属性マップに従って許可されるトンネリング プロトコルであるためです（図 9-9 および図 9-10 を参照）。

図 9-9　クライアントレス ユーザへのログイン拒否メッセージ

図 9-10　AnyConnect クライアント ユーザへのログイン拒否メッセージ



ログイン時間と Time-of-Day ルールの適用

次の例では、クライアントレス SSL ユーザ（たとえばビジネス パートナー）にネットワークへのアクセスを許可する時間帯を設定して適用する方法を示します。

AD サーバ上で、[Office] フィールドを使用してパートナーの名前を入力します。このフィールドでは、physicalDeliveryOfficeName 属性が使用されます。次に、ASA で属性マップを作成し、その属性を Cisco 属性 Access-Hours にマッピングします。認証時に、ASA はサーバから physicalDeliveryOfficeName の値を取得して Access-Hours にマッピングします。

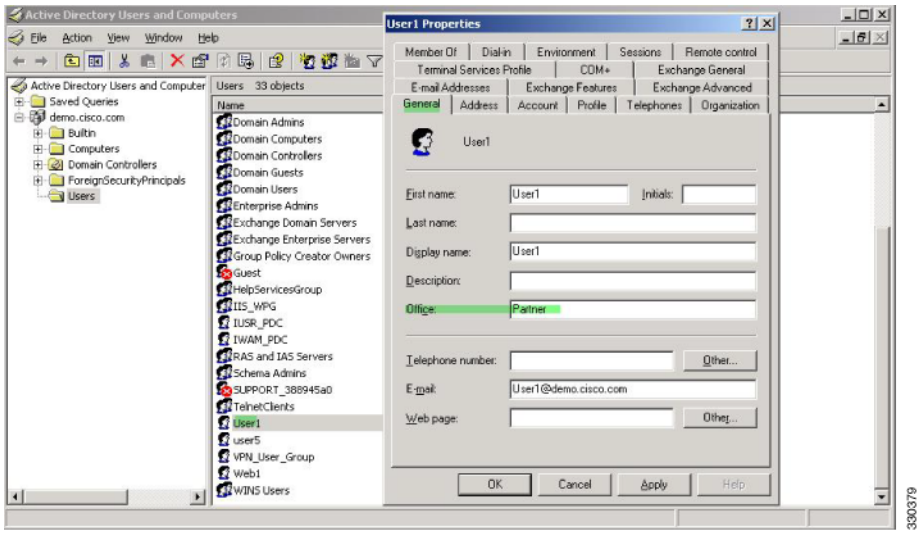
AD/LDAP サーバ上でユーザ属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを選択して [Properties] を右クリックします。

[Properties] ダイアログボックスが表示されます（図 9-11 を参照）。

ステップ 2　[General] タブをクリックします。

図 9-11　Active Directory [Properties] ダイアログボックス



ステップ 3　属性マップを作成します。

次の例では、属性マップ access_hours を作成して AD 属性 physicalDeliveryOfficeName（[Office] フィールドで使用）を Cisco 属性 Access-Hours にマッピングする方法を示します。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ access_hours を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

ステップ 5　各値にサーバで許可された時間範囲を設定します。

次の例では、Partner のアクセス時間が月曜日から金曜日の午前 9 時から午後 5 時に設定されています。

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

ローカル ユーザのグループ ポリシーの作成例

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、一般的な操作のコンフィギュレーション ガイド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、次のトンネリング プロトコルのいずれかを選択します。

- （SSL/TLS を利用する VPN）クライアントレス SSL VPN では、Web ブラウザを使用して VPN コンセントレータへのセキュアなリモート アクセス トンネルを確立し、ソフトウェア クライアントもハードウェア クライアントも必要としません。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
- SSL VPN クライアントは、Cisco AnyConnect Client アプリケーションのダウンロード後にユーザが接続できるようにします。ユーザは、最初にクライアントレス SSL VPN 接続を使用してこのアプリケーションをダウンロードします。ユーザが接続するたびに、必要に応じてクライアント アップデートが自動的に行われます。
- [IPsec IKEv1] : IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2] : AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェア アップデート、クライアント プロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- 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。VPN 3002 の場合、このパラメータは、対話型ハードウェア クライアント認証や個別ユーザ認証には適用されません。

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）　最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

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 分で、最長時間は 2147483647 分（4000 年超、その可能性はほとんどありません）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（オプション）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（オプション）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。

PART 2

クライアントレス SSL VPN

CHAPTER 10

クライアントレス SSL VPN

クライアントレス SSL VPN の概要

クライアントレス SSL VPN を使用すると、エンド ユーザは SSL 対応 Web ブラウザを使用して、任意の場所から社内ネットワークのリソースに安全にアクセスできます。ユーザは、まず、クライアントレス SSL VPN ゲートウェイで認証し、事前設定されたネットワーク リソースにアクセスできるようにします。

（注） クライアントレス SSL VPN がイネーブルになっている場合、セキュリティ コンテキスト（ファイアウォール マルチモードとも呼ばれる）と Active/Active ステートフル フェールオーバーはサポートされません。

クライアントレス SSL VPN は、ソフトウェアまたはハードウェア クライアントを必要とせずに、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを作成します。HTTP 経由でインターネットに接続できるほとんどのデバイスから、幅広い Web リソースと、Web 対応およびレガシー アプリケーションに安全かつ簡単にアクセスできます。次の内容で構成されています。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory ファイル共有
- POP3S、IMAP4S、SMTPS などの電子メール プロキシ
- Microsoft Outlook Web Access Exchange Server 2000、2003、および 2007
- Microsoft Web App to Exchange Server 2010（8.4(2) 以降において）
- Application Access（他の TCP ベースのアプリケーションにアクセスするためのスマート トンネルまたはポート転送）

クライアントレス SSL VPN は Secure Sockets Layer（SSL）プロトコルおよびその後継の Transport Layer Security（SSL/TLS1）を使用して、リモート ユーザと、内部サーバとして設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。ASA はプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、クライアントレス SSL VPN セッションのユーザに対してグループ単位でリソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

前提条件

ASA Release 9.0 でサポートされているプラットフォームおよびブラウザについては、『*Supported VPN Platforms, Cisco ASA Series*』を参照してください。

注意事項と制約事項

- ActiveX ページでは、ActiveX リレーをイネーブルにするか、関連するグループ ポリシーに **activex-relay** を入力しておくことが必要です。あるいは、スマート トンネル リストをポリシーに割り当て、エンドポイント上のブラウザ プロキシ例外リストにプロキシが指定されている場合、ユーザはそのリストに「shutdown.webvpn.relay.」エントリを追加する必要があります。
- ASA では、Windows 7、Vista、Internet Explorer 8 ～ 10、Mac OS X、および Linux から Windows 共有（CIFS）Web フォルダへのクライアントレス アクセスはサポートされていません。
- DoD Common Access Card および SmartCard を含む証明書認証は、Safari キーチェーンだけで動作します。
- ASA は、クライアントレス SSL VPN 接続では DSA または RSA 証明書をサポートしていません。
- 一部のドメインベースのセキュリティ製品には、ASA から送信された要求を超える要件があります。
- コンフィギュレーション制御の検査およびモジュラ ポリシー フレームワークのインスペクション機能はサポートされません。
- NAT および PAT はクライアントに適用可能ではありません。
- クライアントレス SSL VPN のコンポーネントの一部には、Java ランタイム環境（JRE）が必要です。Mac OS X v10.7 以降では Java はデフォルトではインストールされていません。Mac OS X で Java をインストールする方法については、http://java.com/en/download/faq/java_mac.xml を参照してください。

クライアントレス ポータル用に設定された複数のグループ ポリシーがある場合は、ログイン ページのドロップダウンに表示されます。リストにある最初のグループ ポリシーで証明書が必要な場合は、ユーザはマッチング証明書が必要です。グループ ポリシーの一部が証明書を使用しない場合、非証明書ポリシーを最初に表示するには、リストを設定します。また、「0-Select-a-group」の名前でダミー グループ ポリシーを作成することもできます。

ヒント　グループ ポリシーの名前をアルファベット順に付けることで、最初に表示されるポリシーを制御できます。また、ポリシーの先頭に数字を付けることもできます。たとえば、1-AAA、2-Certificate とします。

基本的なクライアントレス SSL VPN のコンフィギュレーション

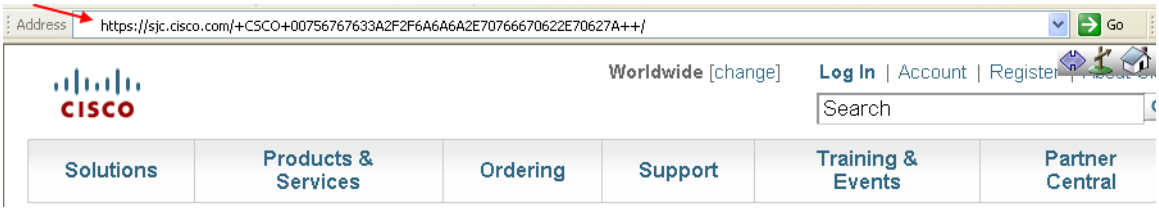
改訂日：2014 年 3 月 12 日

クライアントレス SSL VPN セキュリティ対策

デフォルトでは、ASA はすべての Web リソース（HTTPS、CIFS、RDP、プラグインなど）に対するすべてのポータル トラフィックを許可します。クライアントレス SSL VPN は、ASA だけに意味のあるものに各 URL を書き換えます。ユーザは、要求した Web サイトに接続されていることを確認するために、この URL を使用できません。フィッシング Web サイトからの危険にユーザがさらされるのを防ぐには、クライアントレス アクセスに設定しているポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に Web ACL を割り当ててポータルからのトラフィック フローを制御します。これらのポリシーの URL エントリをオフに切り替えて、何にアクセスできるかについてユーザが混乱しないようにすることをお勧めします。

図 11-1　　ユーザが入力した URL の例

図 11-2　セキュリティ アプライアンスによって書き換えられ、ブラウザ ウィンドウに表示された同じ URL



手順の詳細

ステップ 1　クライアントレス SSL VPN アクセスを必要とするすべてのユーザのグループ ポリシーを設定し、そのグループ ポリシーに対してだけクライアントレス SSL VPN をイネーブルにします。

ステップ 2　グループ ポリシーを開き、[General] > [More Options] > [Web ACL] を選択して [Manage] をクリックします。

ステップ 3　次のいずれかを行う場合、Web ACL を作成します。

- プライベート ネットワーク内の特定のターゲットだけにアクセスを許可する。
- プライベート ネットワークへのアクセスだけを許可する、インターネット アクセスを拒否する、または信頼できるサイトへのアクセスだけを許可する。

ステップ 4　クライアントレス SSL VPN アクセス用に設定しているすべてのポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に Web ACL を割り当てます。Web ACL を DAP に割り当てるには、DAP レコードを編集し、[Network ACL Filters] タブで Web ACL を選択します。

ステップ 5　ブラウザベースの接続の確立時に表示される *ポータル* ページ上の URL エントリをオフに切り替えます。グループ ポリシーのポータル フレームと DAP の [Functions] タブの両方の [URL Entry] の横にある [Disable] をクリックします。DAP 上の URL エントリをオフに切り替えるには、ASDM を使用して DAP レコードを編集し、[Functions] タブをクリックして、[URL Entry] の横にある [Disable] をオンにします。

ステップ 6　ユーザに、ポータル ページの上のネイティブ ブラウザの Address フィールドに外部 URL を入力するか、別のブラウザ ウィンドウを開いて、外部サイトにアクセスするかを指示します。

クライアントレス SSL VPN アクセスの設定

クライアントレス SSL VPN アクセスを設定する場合、次の操作が可能です。

- クライアントレス SSL VPN セッション向けに ASA インターフェイスをイネーブルにする、またはオフに切り替える。
- クライアントレス SSL VPN 接続で使用するポートを選択する。
- 同時クライアントレス SSL VPN セッションの最大数を設定する。

手順の詳細

ステップ 1　クライアントレス アクセス用のグループ ポリシーを設定または作成するには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] ペインを選択します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] の順に進みます。

a. 各 ASA インターフェイスの [Allow Access] をイネーブルにするか、オフに切り替えます。

インターフェイスのカラムには、設定されているインターフェイスのリストが表示されます。[WebVPN Enabled] フィールドに、インターフェイスのクライアントレス SSL VPN のステータスが表示されます。[Yes] の隣に緑のチェックマークが入っていると、クライアントレス SSL VPN はイネーブルになっています。[No] の横の赤色の丸は、クライアントレス SSL VPN がオフに切り替えられていることを示します。

b. [Port Setting] をクリックし、クライアントレス SSL セッションに使用するポート番号（1 ～ 65535）を入力します。デフォルト値は 443 です。ポート番号を変更すると、現在のすべてのクライアントレス SSL VPN 接続が切断されるため、現在のユーザは再接続する必要があります。また、ASDM セッションへの再接続を求めるメッセージが表示されます。

ステップ 3　[Configuration] > [Remote Access VPN] > [Advanced] > [Maximum VPN Sessions] の順に進み、[Maximum Other VPN Sessions] フィールドで許可するクライアントレス SSL VPN セッションの最大数を入力します。

クライアントレス SSL VPN サーバ証明書の確認

クライアントレス SSL VPN 経由でリモート SSL 対応サーバに接続する場合は、リモート サーバを信頼できること、また、接続先が実際にサーバであることを認識することが重要です。ASA 9.0 には、クライアントレス SSL VPN の信頼できる認証局（CA）証明書のリストに対する SSL サーバ証明書の検証のためのサポートが追加されています。

HTTPS プロトコルを使用して Web ブラウザ経由でリモート サーバに接続する場合、サーバはサーバ自体を識別するために認証局（CA）が署名したデジタル証明書を提供します。Web ブラウザには、サーバ証明書の有効性を検証するために使用される一連の CA 証明書が含まれています。これは、公開キー インフラストラクチャ（PKI）の 1 つの形式です。

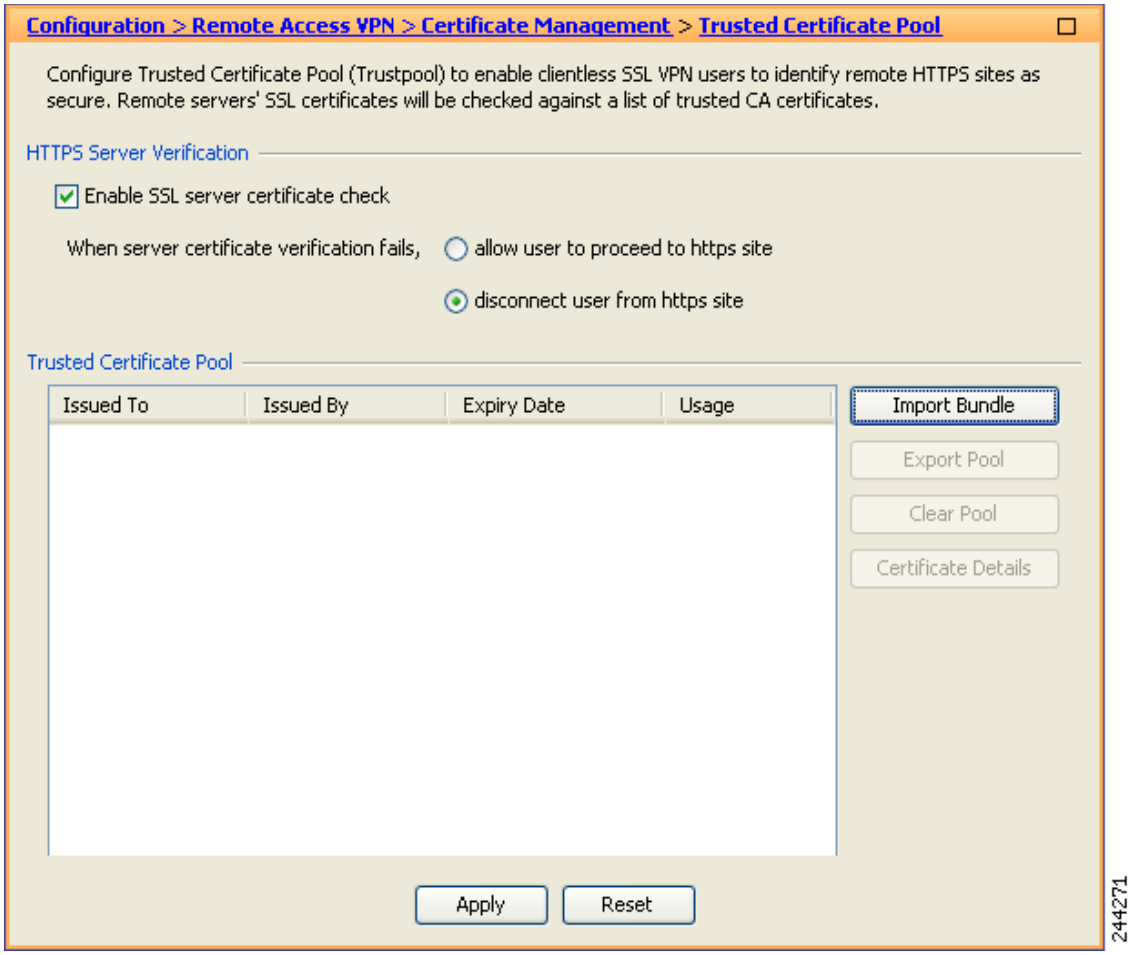
ASA は信頼できるプール証明書の管理機能を trustpool の形式で提供します。これは、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には Web ブラウザに備わっているものと同様のデフォルトの一連の証明書が含まれています。管理者が実行するまでは動作しません。

（注）　ASA trustpool は Cisco IOS trustpool と似ていますが、同じではありません。

HTTP サーバ検証のイネーブル化

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択します。

図 11-3　ASDM での HTTPS サーバ検証のイネーブル化



ステップ 2　[Enable SSL Certificate Check] チェックボックスをオンにします。

ステップ 3　[Disconnect User From HTTPS Site] をクリックして、サーバが検証できなかった場合に切断します。または、[Allow User to Proceed to HTTPS Site] をクリックして、チェックが失敗した場合でも、ユーザが接続を継続できるようにします。

ステップ 4　[Apply] をクリックして変更内容を保存します。

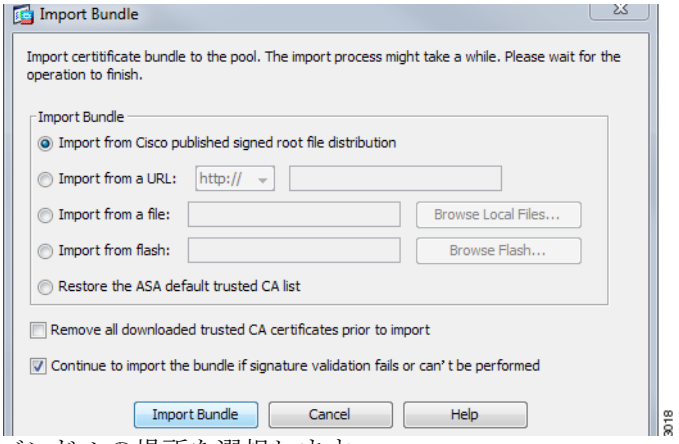
証明書のバンドルのインポート

次の形式のいずれかで、さまざまな場所から個々の証明書または証明書のバンドルをインポートできます。

- pkcs7 構造でラップされた DER 形式の x509 証明書。
- PEM 形式（PEM ヘッダーに囲まれた）の連結した x509 証明書のファイル。

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択します。

ステップ 2　[Import Bundle] をクリックします。



ステップ 3　バンドルの場所を選択します。

- バンドルがコンピュータに保存されている場合は、[Import From a File] をクリックし、[Browse Local Files] をクリックして、バンドルを選択します。
- バンドルが ASA フラッシュ ファイル システムに保存されている場合は、[Import From Flash] をクリックし、[Browse Flash] をクリックして、ファイルを選択します。
- バンドルがサーバでホストされている場合は、[Import From a URL] をクリックして、リストからプロトコルを選択し、フィールドに URL を入力します。
- シグニチャの確認が失敗したり、実行できない場合にバンドルのインポートを継続することにより、バンドルをインポートして、後で個々の証明書のエラーを修正することができます。証明書のいずれかに失敗した場合はバンドル全体が失敗するように、チェックボックスをオフにします。

ステップ 4　[Import Bundle] をクリックします。または、[Cancel] をクリックして変更を破棄します。

（注）　[Remove All Downloaded Trusted CA Certificates Prior to Import] チェックボックスをオンにして、新しいバンドルをインポートする前に trustpool をクリアします。

trustpool のエクスポート

trustpool を正しく設定したら、プールをエクスポートする必要があります。これにより、このポイントまで（たとえばエクスポート後に trustpool に追加された証明書を削除する場合など）trustpool を復元できます。ASA フラッシュ ファイル システムまたはローカル ファイル システムにプールをエクスポートできます。

ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Export Pool] をクリックします。

ステップ 1　[Export to a File] をクリックします。

ステップ 2　[Browse Local Files] をクリックします。

ステップ 3　trustpool を保存するフォルダを選択します。

ステップ 4　[File Name] ボックスに、trustpool の一意の覚えやすい名前を入力します。

ステップ 5　[Select] をクリックします。

ステップ 6　[Export Pool] をクリックして、ファイルを保存します。または、[Cancel] をクリックして保存を停止します。

証明書の削除

すべての証明書を削除するには、ASDM で [Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Clear Pool] をクリックします。

（注）　trustpool をクリアする前に、現在の設定を復元できるように、現在の trustpool をエクスポートする必要があります。

デフォルトの信頼できる認証局リストの復元

デフォルトの信頼できる認証局（CA）リストを復元するには、ASDM で [Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Restore Default Trusted CA List] をクリックし、[Import Bundle] をクリックします。

trustpool の更新

次のいずれかの条件が満たされる場合は、trustpool を更新する必要があります。

- trustpool の証明書が期限切れまたは再発行されている。
- 公開された CA 証明書のバンドルに、特定のアプリケーションで必要な追加の証明書が含まれている。

完全な更新によって、trustpool のすべての証明書が置き換えられます。

実用的な更新では、新しい証明書を追加したり、既存の証明書を置き換えることができます。

証明書のバンドルの削除

trustpool をクリアすると、デフォルトのバンドルではないすべての証明書が削除されます。

デフォルトのバンドルは削除できません。trustpool をクリアするには、ASDM で [Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Clear Pool] をクリックします。

Java Code Signer

コード署名により、デジタル署名が、実行可能なコードそのものに追加されます。このデジタル署名には、さまざまな情報が保持されています。署名以降にそのコードが変更されていないことを保証するだけでなく、署名者を認証する場合に使用することもできます。

コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

Java オブジェクト署名で使用する、設定された証明書をドロップダウン リストから選択します。

Java Code Signer を設定するには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Java Code Signer] を選択します。

クライアントレス SSL VPN が変換した Java オブジェクトは、その後、トラストポイントに関連付けられた PKCS12 デジタル証明書により署名されます。[Java Trustpoint] ペインでは、指定されたトラストポイントの場所から PKCS12 証明書とキー関連情報を使用するようにクライアントレス SSL VPN Java オブジェクト署名機能を設定できます。

トラストポイントをインポートするには、[Configuration] > [Properties] > [Certificate] > [Trustpoint] > [Import] を選択します。

プラグインへのブラウザ アクセスの設定

次の項では、クライアントレス SSL VPN のブラウザ アクセス用のブラウザ プラグインの統合について説明します。

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。ASA により、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

プラグインをフラッシュ デバイスにインストールすると、ASA は次の処理を実行します。

- （シスコが配布したプラグインのみ）URL で指定した jar ファイルを解凍します。
- ASA ファイル システムにファイルを書き込みます。
- ASDM の URL 属性の横にあるドロップダウン リストに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、ポータル ページの [Address] フィールドの横にあるドロップダウン リストにメイン メニュー オプションとオプションを追加します。

表 11-1 に、次の項で説明するプラグインを追加したときの、ポータル ページのメイン メニューと [Address] フィールドの変更点を示します。

* 推奨されないプラグイン。

表 11-1　　クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
ica	Citrix MetaFrame Services	ica://
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	Secure Shell	ssh://
	Telnet services（v1 および v2 をサポート）	telnet://
vnc	Virtual Network Computing services	vnc://

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン リストに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。プラグインは、シングル サインオン（SSO）をサポートします。実装の詳細については、「HTTP Form プロトコルを使用した SSO の設定」（P.15-5）を参照してください。

前提条件

- プラグインへのリモート アクセスを提供するには、ASA でクライアントレス SSL VPN をイネーブルにする必要があります。
- プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマーク エントリを追加します。また、ブックマークを追加するときに、SSO サポートを指定します。
- リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。
- プラグインには、ActiveX または Oracle Java ランタイム環境（JRE）が必要です。バージョン要件については、互換性マトリクスを参照してください。

制約事項

（注） Remote Desktop Protocol プラグインでは、セッション ブローカを使用したロード バランシングはサポートされていません。プロトコルによるセッション ブローカからのリダイレクションの処理方法のため、接続に失敗します。セッション ブローカが使用されていない場合、プラグインは動作します。

- プラグインは、シングル サインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを開くときに入力したクレデンシャルと*同じ*クレデンシャルを使用します。プラグインはマクロ置換をサポートしないため、内部ドメイン パスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。
- ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- ステートフル フェールオーバーではなくステートレス フェールオーバーを使用する場合は、ブックマーク、カスタマイゼーション、ダイナミック アクセス ポリシーなどのクライアントレス機能はフェールオーバー ASA ペア間で同期されません。フェールオーバーの発生時に、これらの機能は動作しません。

プラグインのためのセキュリティ アプライアンスの準備

プラグインをインストールする前に、ASAで次のような準備を行います。

前提条件

クライアントレス SSL VPN が ASA インターフェイスでイネーブルになっていることを確認します。

制約事項

SSL 証明書の一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、ASA と通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

クライアントレス SSL VPN アクセスに提供するプラグインのタイプを指定する項に進んでください。

- 「シスコによって再配布されたプラグインのインストール」（P.11-9）
- 「Citrix XenApp Server へのアクセスの提供」（P.11-11）

シスコによって再配布されたプラグインのインストール

シスコでは、Java ベースのオープン ソース コンポーネントを再配布しています。これは、クライアントレス SSL VPN セッションで Web ブラウザのプラグインとしてアクセスされるコンポーネントで、次のものがあります。

前提条件

ASA のインターフェイス上でクライアントレス SSL VPN がイネーブルになっていることを確認します。そのためには、**show running-config** コマンドを入力します。

表 11-2　　シスコが再配布しているプラグイン

プロトコル	説明	再配布しているプラグインのソース *
RDP	Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。 リモート デスクトップ ActiveX コントロールをサポートします。 RDP および RDP2 の両方をサポートするこのプラグインを使用することをお勧めします。RDP および RDP2 のバージョン 5.1 へのバージョンアップだけがサポートされています。バージョン 5.2 以降はサポートされていません。	http://properjavardp.sourceforge.net/
RDP2	Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。 リモート デスクトップ ActiveX コントロールをサポートします。 **（注）** この古いプラグインは、RDP2 だけをサポートします。このプラグインを使用することは推奨しません。代わりに、上記の RDP プラグインを使用してください。	http://properjavardp.sourceforge.net/
SSH	Secure Shell-Telnet プラグインにより、リモート ユーザはリモート コンピュータへの Secure Shell（v1 または v2）または Telnet 接続を確立できます。 **（注）** キーボード インタラクティブ認証は JavaSSH ではサポートされていないため、（異なる認証メカニズムの実装に使用される）SSH プラグインではサポートされません。	http://javassh.org/
VNC	Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有（VNC サーバまたはサービスとも呼ばれる）をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。このバージョンでは、テキストのデフォルトの色が変更されています。また、フランス語と日本語のヘルプ ファイルもアップデートされています。	http://www.tightvnc.com/

*展開の設定と制限については、プラグインのマニュアルを参照してください。

これらのプラグインは、Cisco Adaptive Security Appliance ソフトウェアのダウンロード サイトで入手できます。

手順の詳細

ステップ 1　ASA との ASDM セッションを確立するために使用するコンピュータに、plugins という名前の一時ディレクトリを作成し、シスコの Web サイトから、必要なプラグインを [plugins] ディレクトリにダウンロードします。

ステップ 2　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Client-Server Plug-ins] を選択します。

このペインには、クライアントレス SSL セッションで使用可能な現在ロードされているプラグインが表示されます。これらのプラグインのハッシュおよび日付も表示されます。

ステップ 3　[Import] をクリックします。

[Import Client-Server Plug-in] ダイアログボックスが開きます。

ステップ 4　[Import Client-Server Plug-in] ダイアログボックスのフィールド値を入力するには、次の説明を参考にしてください。

- [Plug-in Name]：次のいずれかの値を入力します。
  - **ica**。Citrix MetaFrame または Web Interface サービスへのプラグイン アクセスを提供する場合に指定します。
  - Remote Desktop Protocol サービスへのプラグイン アクセスを提供するには、**rdp** を入力します。
  - セキュア シェル サービスと Telnet サービスの*両方*にプラグイン アクセスを提供するには、**ssh,telnet** を入力します。
  - Virtual Network Computing サービスにプラグイン アクセスを提供するには、**vnc** を入力します。

（注）　このメニューの、記載のないオプションは実験的なものであるため、サポートされていません。

- [Select the location of the plugin file]：次のいずれかのオプションをクリックし、テキスト フィールドにパスを挿入します。
  - [Local computer]：関連する [Path] フィールドにプラグインの場所と名前を入力するか、[Browse Local Files] をクリックしてプラグインを選択し、プラグインを選択して [Select] をクリックします。
  - [Flash file system]：関連する [Path] フィールドにプラグインの場所と名前を入力するか、[Browse Flash] をクリックしてプラグインを選択し、プラグインを選択して [OK] をクリックします。
  - [Remote Server]：リモート サーバで実行されているサービスに応じて、関連付けられた [Path] 属性の横にあるドロップダウン メニューで [ftp]、[tftp]、または [HTTP] を選択します。隣にあるテキスト フィールドに、サーバのホスト名またはアドレスおよびプラグインへのパスを入力します。

ステップ 5　[Import Now] をクリックします。

ステップ 6　[Apply] をクリックします。

これで、以降のクライアントレス SSL VPN セッションでプラグインが使用できるようになりました。

Citrix XenApp Server へのアクセスの提供

サードパーティのプラグインに、クライアントレス SSL VPN ブラウザ アクセスを提供する方法の例として、この項では、Citrix XenApp Server Client にクライアントレス SSL VPN のサポートを追加する方法について説明します。

ASA に Citrix プラグインがインストールされている場合、クライアントレス SSL VPN ユーザは、ASA への接続を使用して、Citrix XenApp サービスにアクセスできます。

ステートフル フェールオーバーでは、Citrix プラグインを使用して確立したセッションは保持されません。Citrix のユーザは、フェールオーバー後に再認証を行う必要があります。

Citrix プラグインへのアクセスを提供するには、次の項で説明する手順に従ってください。

- 「クライアントレス SSL VPN アクセスのための Citrix XenApp Server の準備」
- 「Citrix プラグインの作成とインストール」

クライアントレス SSL VPN アクセスのための Citrix XenApp Server の準備

（Citrix）「セキュア ゲートウェイ」を使用しないモードで動作するように、Citrix Web Interface ソフトウェアを設定する必要があります。この設定をしないと、Citrix クライアントは Citrix XenApp Server に接続できません。

（注） プラグインに対するサポートをまだ提供していない場合は、「プラグインのためのセキュリティ アプライアンスの準備」（P.11-8）の説明に従い作業を行った後に、この項を参照してください。

Citrix プラグインの作成とインストール

手順の詳細

ステップ 1　シスコのソフトウェア ダウンロード Web サイトから ica-plugin.zip ファイルをダウンロードします。

このファイルには、Citrix プラグインを使用するためにシスコがカスタマイズしたファイルが含まれています。

ステップ 2　Citrix のサイトから Citrix Java クライアントをダウンロードします。

Citrix Web サイトのダウンロード領域で [Citrix Receiver]、[Receiver for Other Platforms] を選択し、[Find] をクリックします。[Receiver for Java] ハイパーリンクをクリックしアーカイブをダウンロードします。

ステップ 3　アーカイブから次のファイルを抽出し、それらを ica-plugin.zip ファイルに追加します。

- JICA-configN.jar
- JICAEngN.jar

ステップ 4　Citrix Java クライアントに含まれている EULA によって、Web サーバ上にクライアントを配置するための権限が与えられていることを確認します。

ステップ 5　ASDM を使用するか、または特権 EXEC モードで次の CLI コマンドを入力して、プラグインをインストールします。

import webvpn plug-in protocol ica *URL*

URL はホスト名または IP アドレス、および ica-plugin.zip ファイルへのパスです。

（注）　Citrix セッションに SSO サポートを提供する場合は、ブックマークの追加は必須です。次のように、ブックマークで便利な表示を提供する URL パラメータを使用することを推奨します。

ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

ステップ 6　SSL VPN クライアントレス セッションを確立し、ブックマークをクリックするか、Citrix サーバの URL を入力します。

必要に応じて、『Client for Java Administrator's Guide』を参照してください。

ポート転送の設定

次の項では、ポート転送とその設定方法について説明します。

ポート転送に関する情報

ポート転送により、ユーザはクライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションにアクセスできます。TCP ベースのアプリケーションには次のようなものがあります。

- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP（FTP over SSH）
- SSH
- Telnet
- Windows Terminal Service
- XDDTS

その他の TCP ベースのアプリケーションも動作する可能性はありますが、シスコではテストを行っていません。UDP を使用するプロトコルは動作しません。

ポート転送は、クライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションをサポートするためのレガシー テクノロジーです。ポート転送テクノロジーをサポートする設定を事前に構築している場合は、ポート転送の使用を選択することもできます。

ポート転送の代替方法として次のことを検討してください。

- スマート トンネル アクセスを使用すると、ユーザには次のような利点があります。
  - スマート トンネルは、プラグインよりもパフォーマンスが向上します。
  - ポート転送とは異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続を要求しないことにより、ユーザ エクスペリエンスが簡略化されます。
  - ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。
- ポート転送およびスマート トンネル アクセスとは異なり、プラグインでは、クライアント アプリケーションをリモート コンピュータにインストールする必要がありません。

ASA でポート転送を設定する場合は、アプリケーションが使用するポートを指定します。スマート トンネル アクセスを設定する場合は、実行ファイルまたはそのパスの名前を指定します。

前提条件

- リモート ホストで、次のいずれかの 32 ビット バージョンが実行されている必要がある。
  - Microsoft Windows Vista、Windows XP SP2 または SP3、または Windows 2000 SP4
  - Apple Mac OS X 10.4 または 10.5 と Safari 2.0.4(419.3)
  - Fedora Core 4
- また、リモート ホストで Oracle Java ランタイム環境（JRE）5 以降が動作している必要もある。
- Mac OS X 10.5.3 上の Safari のブラウザベースのユーザは、Safari での URL の解釈方法に従って、使用するクライアント証明書を、1 回目は末尾にスラッシュを含め、もう 1 回はスラッシュを含めずに、ASA の URL を使用して指定する必要があります。次に例を示します。
  - https://example.com/
  - https://example.com

  詳細については、『Safari, Mac OS X 10.5.3: Changes in client certificate authentication』を参照してください。
- ポート転送またはスマート トンネルを使用する Microsoft Windows Vista 以降のユーザは、ASA の URL を信頼済みサイト ゾーンに追加する。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動し、[Tools] > [Internet Options] > [Security] タブを選択する必要があります。Vista（以降の）ユーザは保護モードをオフに切り替えるとスマート トンネル アクセスを使用することもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法の使用はお勧めしません。
- ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートするために、リモート コンピュータに Oracle Java ランタイム環境（JRE）1.5.x 以降がインストールされていることを確認します。JRE 1.4.x が実行中で、ユーザがデジタル証明書で認証される場合、JRE が Web ブラウザの証明書ストアにアクセスできないため、アプリケーションは起動しません。

制約事項

- ポート転送は、スタティック TCP ポートを使用する TCP アプリケーションのみをサポートしています。ダイナミック ポートまたは複数の TCP ポートを使用するアプリケーションはサポートしていません。たとえば、ポート 22 を使用する SecureFTP は、クライアントレス SSL VPN のポート転送を介して動作しますが、ポート 20 と 21 を使用する標準 FTP は動作しません。
- ポート転送は、UDP を使用するプロトコルをサポートしていません。
- ポート転送は Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。しかし、Microsoft Outlook Exchange Server と連携することにより、Microsoft Office Outlook のスマート トンネル サポートを設定することができます。
- ステートフル フェールオーバーでは、Application Access（ポート転送またはスマート トンネル アクセス）を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- ポート転送は、携帯情報端末（PDA）への接続はサポートしていません。
- ポート転送を使用するには、Java アプレットをダウンロードしてローカル クライアントを設定する必要があります。これには、ローカル システムに対する管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

  Java アプレットは、エンド ユーザの HTML インターフェイスにあるアプレット独自のウィンドウに表示されます。このウィンドウには、ユーザが使用できる転送ポートのリストの内容、アクティブなポート、および送受信されたトラフィック量（バイト単位）が表示されます。
- ローカル IP アドレス 127.0.0.1 が使用されており、ASA からのクライアントレス SSL VPN 接続によって更新できない場合、ポート転送アプレットはローカル ポートとリモート ポートを同一として表示します。その結果、ASA は、127.0.0.2、127.0.0.3 など、ローカル プロキシ ID の新しい IP アドレスを作成します。hosts ファイルを変更して異なるループバックを使用できるため、リモート ポートはアプレットでローカル ポートとして使用されます。接続するには、ポートを指定せずにホスト名を指定して Telnet を使用します。正しいローカル IP アドレスをローカル ホスト ファイルで使用できます。

ポート転送用の DNS の設定

ポート転送では、リモート サーバのドメイン名またはその IP アドレスを ASA に転送して、解決および接続を行います。つまり、ポート転送アプレットは、アプリケーションからの要求を受け入れて、その要求を ASA に転送します。ASA は適切な DNS クエリーを作成し、ポート転送アプレットの代わりに接続を確立します。ポート転送アプレットは、ASA に対する DNS クエリーだけを作成します。ポート転送アプレットはホスト ファイルをアップデートして、ポート転送アプリケーションが DNS クエリーを実行したときに、クエリーがループバック アドレスにリダイレクトされるようにします。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] の順にクリックします。

デフォルトのクライアントレス SSL VPN グループ エントリは、クライアントレス接続に使用されるデフォルトの接続プロファイルです。

ステップ 2　設定をクライアントレス接続にも使用する場合は、デフォルトのクライアントレス SSL VPN グループ エントリを強調表示し、[Edit] をクリックします。このエントリが使用されない場合は、クライアント接続のコンフィギュレーションで使用される接続プロファイルを強調表示し、[Edit] をクリックします。

[Basic] ウィンドウが開きます。

ステップ 3　[DNS] 領域にスキャンし、ドロップダウン リストから DNS サーバを選択します。ドメイン名をメモしておきます。使用する DNS サーバが ASDM に表示されている場合は、残りのステップを飛ばし、次のセクションに移動します。ポート転送リストのエントリを設定する際、リモート サーバの指定時には、同じドメイン名を入力する必要があります。コンフィギュレーションに DNS サーバがない場合は、残りのステップを続けます。

ステップ 4　[DNS] 領域で [Manage] をクリックします。

[Configure DNS Server Groups] ウィンドウが開きます。

ステップ 5　[Configure Multiple DNS Server Groups] をクリックします。

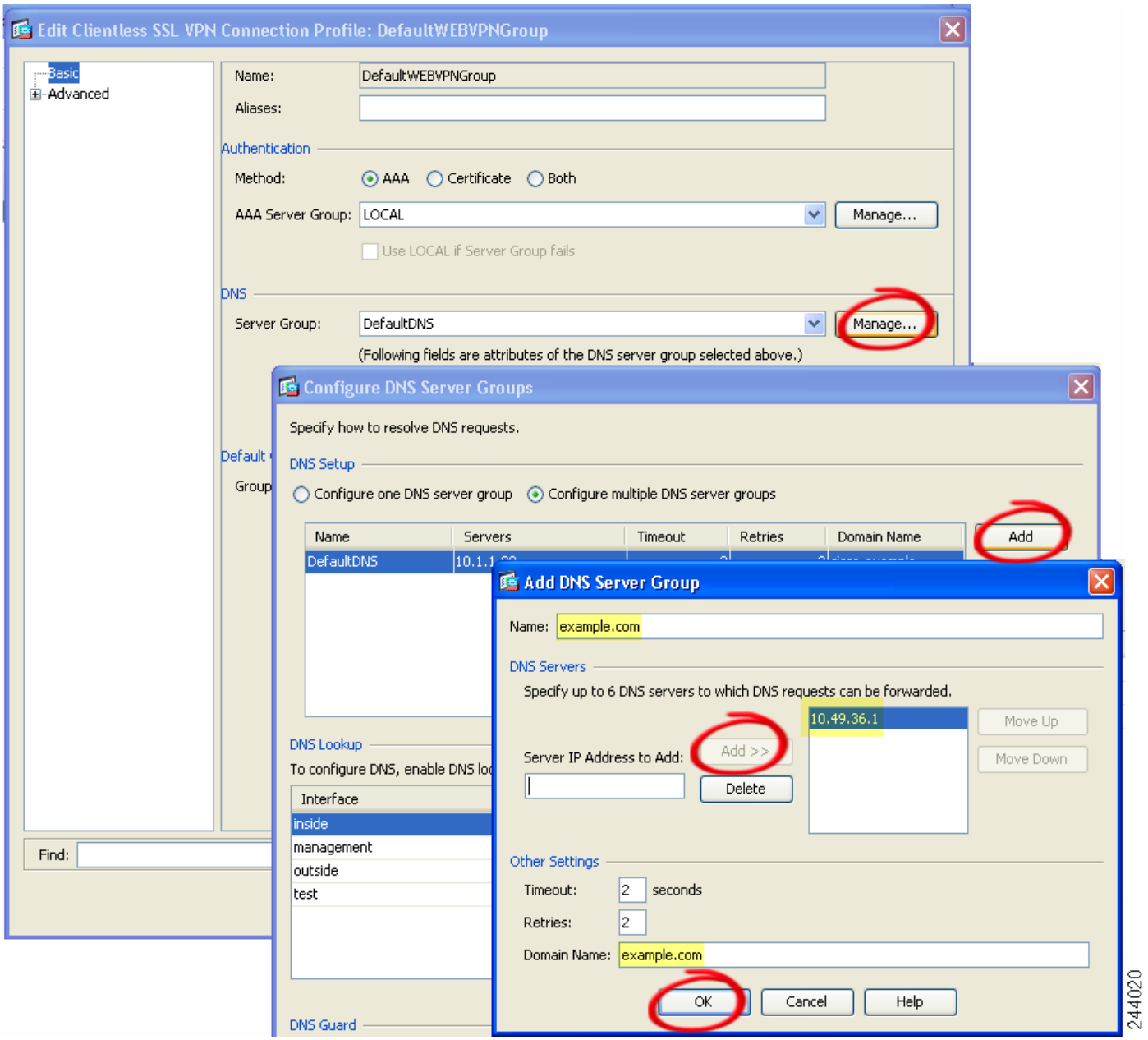
ウィンドウに、DNS サーバのエントリの一覧表が表示されます。

ステップ 6　[Add] をクリックします。

[Add DNS Server Group] ウィンドウが開きます。

ステップ 7　[Name] フィールドに新しいサーバ グループ名を入力し、IP アドレスとドメイン名を入力します（図 11-4 を参照）。

図 11-4　　ポート転送の DNS サーバ値の例



入力したドメイン名を書き留めます。後ほど、ポート転送エントリを設定する際、リモートサーバを指定するために必要になります。

ステップ 8　[Connection Profiles] ウィンドウが再度アクティブになるまで、[OK] をクリックします。

ステップ 9　クライアントレス接続の設定で使用される、残りすべての接続プロファイルについて、手順 2 ～8 を繰り返します。

ステップ 10　[Apply] をクリックします。

アプリケーションのポート転送適格化

各 ASA のクライアントレス SSL VPN コンフィギュレーションは、*ポート転送リスト*をサポートしています。それぞれのリストでは、アクセスを提供するアプリケーションが使用するローカル ポートとリモート ポートを指定します。各グループ ポリシーまたはユーザ名は 1 つのポート転送リストのみをサポートするため、サポートされる CA のセットをグループ化してリストを作成する必要があります。ASA コンフィギュレーションにすでに存在するポート転送リストのエントリを表示するには、次のコマンドを入力します。

ポート転送リストの設定に続けて、次の項で説明するように、そのリストをグループ ポリシーまたはユーザ名に割り当てます。

ポート転送エントリの追加と編集

[Add/Edit Port Forwarding Entry] ダイアログボックスでは、クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションを指定できます。これらのウィンドウで属性に値を割り当てるには、次の手順を実行します。

前提条件

トンネルを確立し、IP アドレスに解決するには、「ポート転送リストの割り当て」（P.11-18）に記載のとおり、[Remote Server] パラメータに割り当てた DNS 名が、[Domain Name] および [Server Group] パラメータと一致する必要があります。[Domain] および [Server Group] パラメータのデフォルト設定は、いずれも DefaultDNS です。

手順の詳細

ステップ 1　[Add] をクリックします。

ステップ 2　アプリケーションが使用する TCP ポート番号を入力します。ローカル ポート番号は、1 つの listname に対して一度だけ使用できます。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

ステップ 3　リモート サーバのドメイン名または IP アドレスを入力します。特定の IP アドレスに対してクライアント アプリケーションを設定しなくて済むよう、ドメイン名を使用することをお勧めします。

ステップ 4　そのアプリケーション用の well-known ポート番号を入力します。

ステップ 5　アプリケーションの説明を入力します。最大で 64 文字まで指定可能です。

ステップ 6　（オプション）ポート転送リストを強調表示し、[Assign] をクリックして、選択したリストを 1 つ以上のグループ ポリシー、ダイナミック アクセス ポリシー、またはユーザ ポリシーに割り当てます。

ポート転送リストの割り当て

クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションの名前付きリストを追加または編集できます。グループ ポリシーとユーザ名ごとに、次のいずれかを行うようにクライアントレス SSL VPN を設定できます。

- ユーザのログイン時に自動的にポート転送アクセスを開始する。
- ユーザのログイン時にポート転送アクセスをイネーブル化するが、クライアントレス SSL VPN ポータル ページの [Application Access] > [Start Applications] を使用して、ポート転送を手動で開始するようにユーザに要求する。

（注） これらのオプションは、各グループ ポリシーとユーザ名に対して互いに排他的です。1 つだけ使用してください。

手順の詳細

[Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックスでは、次のものを追加または編集できます。

ステップ 1　リストの英数字の名前を指定します。最大で 64 文字まで指定可能です。

ステップ 2　アプリケーションのトラフィックを受信するローカル ポートを入力します。ローカル ポート番号は、1 つの listname に対して一度だけ使用できます。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

（注） リモート サーバの IP アドレスまたは DNS 名を入力します。特定の IP アドレスに対してクライアント アプリケーションを設定しなくて済むよう、ドメイン名を使用することをお勧めします。

ステップ 3　アプリケーションのトラフィックを受信するリモート ポートを入力します。

ステップ 4　TCP アプリケーションの説明を入力します。最大で 64 文字まで指定可能です。

ポート転送のイネーブル化と切り替え

デフォルトでは、ポート転送はオフになっています。

ポート転送をイネーブルにした場合、ユーザはクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Applications] を使用して、ポート転送を手動で開始する必要があります。

ファイル アクセスの設定

クライアントレス SSL VPN は、リモート ユーザに HTTPS ポータル ページを提供しています。このページは、ASA で実行するプロキシ CIFS クライアントまたは FTP クライアント（あるいはその両方）と連動しています。クライアントレス SSL VPN は、CIFS または FTP を使用して、ユーザが認証の要件を満たしているファイルのプロパティがアクセスを制限しない限り、ネットワーク上のファイルへのネットワーク アクセスをユーザに提供します。CIFS クライアントおよび FTP クライアントは透過的です。クライアントレス SSL VPN から送信されるポータル ページでは、ファイル システムに直接アクセスしているかのように見えます。

ユーザがファイルのリストを要求すると、クライアントレス SSL VPN は、そのリストが含まれるサーバの IP アドレスをマスター ブラウザに指定されているサーバに照会します。ASA はリストを入手してポータル ページ上のリモート ユーザに送信します。

クライアントレス SSL VPN は、ユーザの認証要件とファイルのプロパティに応じて、ユーザが次の CIFS および FTP の機能を呼び出すことができるようにします。

- ドメインとワークグループ、ドメインまたはワークグループ内のサーバ、サーバ内部の共有、および共有部分またはディレクトリ内のファイルのナビゲートとリスト。
- ディレクトリの作成。
- ファイルのダウンロード、アップロード、リネーム、移動、および削除。

ASA は、通常、ASA と同じネットワーク上か、またはこのネットワークからアクセス可能な場所のマスター ブラウザ、WINS サーバ、または DNS サーバを使用して、リモート ユーザがクライアントレス SSL VPN セッション中に表示されるポータル ページのメニュー上またはツールバー上の [Browse Networks] をクリックしたときに、ネットワークでサーバのリストを照会します。

マスター ブラウザまたは DNS サーバは、ASA 上の CIFS/FTP クライアントに、クライアントレス SSL VPN がリモート ユーザに提供する、ネットワーク上のリソースのリストを表示します。

（注） ファイル アクセスを設定する前に、ユーザ アクセス用のサーバに共有を設定する必要があります。

CIFS ファイル アクセスの要件と制限事項

`\\server\share\subfolder\personal` ***フォルダ***にアクセスするには、最低限、共有自体を含むすべての親フォルダに対する読み取り権限がユーザに必要です。

CIFS ディレクトリとローカル デスクトップとの間でファイルをコピー アンド ペーストするには、[Download] または [Upload] を使用します。[Copy] ボタンおよび [Paste] ボタンはリモート間のアクションのみで使用でき、ローカルからリモートまたはリモートからローカルへのアクションには使用できません。

CIFS ブラウズ サーバ機能は、2 バイト文字の共有名（13 文字を超える共有名）をサポートしていません。これは、表示されるフォルダのリストに影響を与えるだけで、フォルダへのユーザ アクセスには影響しません。回避策として、2 バイトの共有名を使用する CIFS フォルダのブックマークを事前に設定するか、ユーザが cifs://server/<long-folder-name> 形式でフォルダの URL またはブックマークを入力します。次に例を示します。

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

ファイル アクセスのサポートの追加

次の手順を実行して、ファイル アクセスを設定します。

（注）　この手順では、マスター ブラウザおよび WINS サーバを指定する方法について説明します。代わりに、ASDM を使用して、ファイル共有へのアクセスを提供する URL リストとエントリを設定することもできます。

ASDM での共有の追加には、マスター ブラウザまたは WINS サーバは必要ありません。ただし、Browse Networks リンクへのサポートは提供されません。**nbns-server** コマンドを入力するときは、ホスト名または IP アドレスを使用して ServerA を参照できます。ホスト名を使用する場合、ASA はホスト名を IP アドレスに解決するように DNS サーバに要求します。

これらのコマンドの詳しい説明については、コマンド リファレンスを参照してください。

SharePoint アクセスのためのクロックの精度の確認

ASA のクライアントレス SSL VPN サーバは、クッキーを使用して、エンドポイントの Microsoft Word などのアプリケーションと対話します。ASA で設定されたクッキーの有効期間により、ASA の時間が正しくない場合、SharePoint サーバ上の文書にアクセスするときに Word が正しく機能しなくなる可能性があります。このような誤作動を回避するには、ASA クロックを正しく設定します。NTP サーバとダイナミックに同期化されるように ASA を設定することをお勧めします。手順については、一般的な操作のコンフィギュレーション ガイドの日付と時刻の設定の項を参照してください。

仮想デスクトップ インフラストラクチャ（VDI）

ASA は、Citrix サーバおよび VMware VDI サーバへの接続をサポートします。

- Citrix の場合、ASA ではクライアントレス ポータルを介してユーザの実行中の Citrix Receiver へアクセスできます。
- VMware は、（スマート トンネル）のアプリケーションとして設定されます。

VDI サーバには、他のサーバ アプリケーションなど、クライアントレス ポータルのブックマークを介してアクセスできます。

制限事項

- 自動サインオンの場合、証明書またはスマート カードを使用する認証はサポートされません。これは、これらの認証形式では間にある ASA を許可しないためです。
- XML サービスは XenApp サーバおよび XenDesktop サーバにインストールし、設定する必要があります。
- スタンドアロン モバイル クライアントを使用している場合は、クライアント証明書の確認、二重認証、内部パスワードと CSD（Vault だけでなく、すべての CSD）はサポートされません。

Citrix モバイルのサポート

Citrix Receiver を実行しているモバイル ユーザは、次を実行して Citrix サーバに接続できます。

- AnyConnect で ASA に接続してから Citrix サーバに接続する。
- AnyConnect クライアントを使用せずに ASA を介して Citrix サーバに接続する。ログオン クレデンシャルには次を含めることができます。
  - Citrix ログオン画面の接続プロファイルのエイリアス（トンネル グループ エイリアスとも呼ばれる）。VDI サーバは、それぞれ別の権限と接続設定を備えた複数のグループ ポリシーを持つことができます。
  - RSA サーバが設定されている場合は RSA SecureID トークンの値。RSA サポートには、無効なエントリ用の次のトークンと、最初の PIN または期限切れ PIN 用の新しい PIN を入力するための次のトークンが含まれています。

サポートされているモバイル デバイス

- iPad：Citrix Receiver バージョン 4.x 以降
- iPhone/iTouch：Citrix Receiver バージョン 4.x 以降
- Android 2.x/3.x/4.0/4.1 電話機：Citrix Receiver バージョン 2.x 以降
- Android 4.0 電話機：Citrix Receiver バージョン 2.x 以降

制限事項

証明書の制限

- 証明書/スマート カード認証は自動サインオンの手段としてはサポートされていません。
- クライアント証明書の確認および CSD はサポートされていません。
- 証明書の Md5 署名は、iOS の既知の問題であるセキュリティ上の問題（http://support.citrix.com/article/CTX132798）から動作していません。
- SHA2 シグニチャは Citrix Web サイト（http://www.citrix.com/）の説明に従って Windows を除き、サポートされていません。
- 1024 以上のキーサイズはサポートされていません。

その他の制限

- HTTP リダイレクトはサポートされません。Citrix Receiver アプリケーションはリダイレクトでは機能しません。。
- XML サービスは XenApp サーバおよび XenDesktop サーバにインストールし、設定する必要があります。

Citrix Mobile Receiver のユーザ ログオンについて

Citrix サーバに接続しているモバイル ユーザのログオンは、ASA が Citrix サーバを VDI サーバとして設定したか、または VDI プロキシ サーバとして設定したかによって異なります。

Citrix サーバが VDI サーバとして設定されている場合：

1. AnyConnect セキュア モビリティ クライアントを使用し、VPN クレデンシャルで ASA に接続します。
2. Citrix Mobile Receiver を使用し、Citrix サーバ クレデンシャルで Citrix サーバに接続します（シングル サインオンを設定している場合は、Citrix クレデンシャルは不要です）。

ASA が VDI プロキシ サーバとして設定されている場合：

1. Citrix Mobile Receiver を使用し、VPN と Citrix サーバの両方のクレデンシャルを入力して ASA に接続します。最初の接続後、正しく設定されている場合は、以降の接続に必要なのは VPN クレデンシャルだけです。

Citrix サーバをプロキシする ASA の設定

ASA を Citrix サーバのプロキシとして動作するように設定し、ASA への接続が Citrix サーバへの接続であるかのようにユーザに見せることができます。ASDM の VDI プロキシがイネーブルになっている場合は AnyConnect クライアントは不要です。次の手順は、エンド ユーザから Citrix に接続する方法の概要を示します。

1. モバイル ユーザが Citrix Receiver を起動し、ASA の URL に接続します。
2. Citrix のログイン画面で、XenApp サーバのクレデンシャルと VPN クレデンシャルを指定します。
3. 以降、Citrix サーバに接続する場合に必要になるのは、VPN クレデンシャルだけです。

XenDesktop および XenApp のプロキシとして ASA を使用すると Citrix Access Gateway は必要なくなります。XenApp サーバ情報が ASA に記録され、ASDM に表示されます。

Citrix サーバのアドレスおよびログイン クレデンシャルを設定し、グループ ポリシーまたはユーザ名にその VDI サーバを割り当てます。ユーザ名とグループ ポリシーの両方を設定した場合は、ユーザ名の設定によってグループ ポリシー設定がオーバーライドされます。

その他の情報

http://www.youtube.com/watch?v=JMM2RzppaG8：このビデオでは、その ASA を Citrix プロキシとして使用する利点について説明します。

VDI サーバの設定

1 サーバの場合：

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] を選択します。
2. [Enable VDI Server Proxy] チェックボックスをオンにし、VDI サーバを設定します。

複数のグループ ポリシーを VDI サーバに割り当てる場合：

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] を選択します。
2. [Configure All VDI Servers] チェックボックスをオンにします。
3. VDI サーバを追加し、1 つ以上のグループ ポリシーを割り当てます。

VDI プロキシ サーバの設定

1 グループ ポリシーが割り当てられた 1 つの VDI サーバ：

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] を選択します。
2. [Enable VDI Server Proxy] チェックボックスをオンにし、VDI サーバを設定します。

複数のグループ ポリシーを VDI サーバに割り当てる場合：

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] の順に移動します。
2. [Configure All VDI Servers] チェックボックスをオンにします。
3. VDI サーバを追加し、1 つ以上のグループ ポリシーを割り当てます。

グループ ポリシーへの VDI サーバの割り当て

VDI サーバを設定し、グループ ポリシーに割り当てる方法は次のとおりです。

- [VDI Access] ペインで VDI サーバを追加し、サーバにグループ ポリシーを割り当てる。
- グループ ポリシーに VDI サーバを追加する。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] を参照します。

ステップ 2　DfltGrpPolicy を編集し、左側のメニューから [More Options] メニューを展開します。

ステップ 3　[VDI Access] を選択します。[Add] または [Edit] をクリックして、VDI サーバの詳細を表示します。

- [Server (Host Name or IP Address)]：XenApp または XenDesktop サーバのアドレス。この値は、クライアントレス マクロにすることができます。
- [Port Number (Optional)]：Citrix サーバに接続するためのポート番号。この値は、クライアントレス マクロにすることができます。
- [Active Directory Domain Name]：仮想化インフラストラクチャ サーバにログインするためのドメイン。この値は、クライアントレス マクロにすることができます。
- [Use SSL Connection]：サーバに SSL を使用して接続する場合、チェックボックスをオンにします。
- [Username]：仮想化インフラストラクチャ サーバにログインするためのユーザ名。この値は、クライアントレス マクロにすることができます。
- [Password]：仮想化インフラストラクチャ サーバにログインするためのパスワード。この値は、クライアントレス マクロにすることができます。

	コマンド	目的
ステップ 1	`webvpn`	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	`url-entry disable`	URL エントリをオフに切り替えます。

クライアント/サーバ プラグインへのブラウザ アクセスの設定

[Client-Server Plug-in] テーブルには、ASA によってクライアントレス SSL VPN セッションのブラウザで使用できるようになるプラグインが表示されます。

プラグインを追加、変更、または削除するには、次のいずれかを実行します。

- プラグインを追加するには、[Import] をクリックします。[Import Plug-ins] ダイアログボックスが開きます。

プラグインを削除するには、そのプラグインを選択して [Delete] をクリックします。次の項では、クライアントレス SSL VPN のブラウザ アクセス用のブラウザ プラグインの統合について説明します。

- ブラウザ プラグインのインストールについて
- プラグインのためのセキュリティ アプライアンスの準備
- シスコによって再配布されたプラグインのインストール

ブラウザ プラグインのインストールについて

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。ASA により、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

プラグインをフラッシュ デバイスにインストールすると、ASA は次の処理を実行します。

- （シスコが配布したプラグインのみ）*URL* で指定した jar ファイルを解凍します。
- ASA ファイル システムの csco-config/97/plugin ディレクトリにファイルを書き込みます。
- ASDM の URL 属性の横にあるドロップダウン リストに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、ポータル ページの [Address] フィールドの横にあるドロップダウン リストにメイン メニュー オプションとオプションを追加します。

  表 11-3 に、次の項で説明するプラグインを追加したときの、ポータル ページのメイン メニューと [Address] フィールドの変更点を示します。

表 11-3　クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

（注）　セカンダリ ASA は、プライマリ ASA からプラグインを取得します。

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン リストに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

（注）　Java プラグインによっては、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインというステータスがレポートされることがあります。open-source プラグインは、ASA ではなくステータスをレポートします。

1 つ目のプラグインをインストールする前に、次の項の指示に従う必要があります。

前提条件

- セキュリティ アプライアンスでクライアントレス セッションがプロキシ サーバを使用するように設定している場合、プラグインは機能しません。

（注）　Remote Desktop Protocol プラグインでは、セッション ブローカを使用したロード バランシングはサポートされていません。プロトコルによるセッション ブローカからのリダイレクションの処理方法のため、接続に失敗します。セッション ブローカが使用されていない場合、プラグインは動作します。

- プラグインは、シングル サインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを開くときに入力したクレデンシャルと*同じ*クレデンシャルを使用します。プラグインはマクロ置換をサポートしないため、内部ドメイン パスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。
- プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマーク エントリを追加します。また、ブックマークを追加するときに、SSO サポートを指定します。
- リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。

要件

- シスコでは、GNU 一般公的使用許諾（GPL）に従い、変更を加えることなくプラグインを再配布しています。GPL により、これらのプラグインを直接改良できません。
- プラグインへのリモート アクセスを提供するには、ASA でクライアントレス SSL VPN をイネーブルにする必要があります。
- ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- プラグインには、ActiveX または Oracle Java ランタイム環境（JRE）1.4.2（以降）がブラウザでイネーブルになっている必要があります。64 ビット ブラウザには、RDP プラグインの ActiveX バージョンはありません。

RDP プラグイン ActiveX デバッグのクイック リファレンス

RDP プラグインをセットアップして使用するには、新しい環境変数を追加する必要があります。

ステップ 1　[My Computer] を右クリックし、[System Properties] を開いて [Advanced] タブを選択します。

ステップ 2　[Advanced] タブで、[Environment Variables] ボタンを選択します。

ステップ 3　[New User Variable] ダイアログボックスで、RF_DEBUG 変数を入力します。

ステップ 4　[User variables] セクションの新しい環境変数を確認します。

ステップ 5　バージョン 8.3 の前にクライアントレス SSL VPN のバージョンでクライアント コンピュータを使用していた場合、古い Cisco Portforwarder Control を削除してください。C:/WINDOWS/Downloaded Program Files ディレクトリを開いて、Portforwarder Control を右クリックして、[Remove] を選択します。

ステップ 6　Internet Explorer ブラウザのすべてのキャッシュをクリアします。

ステップ 7　クライアントレス SSL VPN セッションを起動して、RDP ActiveX プラグインを使用して RDP セッションを確立します。

これで Windows アプリケーションのイベント ビューアでイベントを確認できるようになります。

プラグインのためのセキュリティ アプライアンスの準備

ステップ 1　クライアントレス SSL VPN が ASA インターフェイスでイネーブルになっていることを確認します。

ステップ 2　リモート ユーザが完全修飾ドメイン名（FQDN）を使用して接続する ASA インターフェイスに SSL 証明書をインストールします。

（注）　SSL 証明書の一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、ASA と通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

CHAPTER 12

高度なクライアントレス SSL VPN のコンフィギュレーション

Microsoft Kerberos Constrained Delegation ソリューション

多くの組織では、現在 ASA SSO 機能によって提供される以上の認証方式を使用して、クライアントレス VPN ユーザを認証し、ユーザの認証クレデンシャルを Web ベースのリソースにシームレスに拡張する必要があります。スマート カードおよびワンタイム パスワード（OTP）を使用したリモート アクセス ユーザの認証に対する要求が大きくなっていますが、SSO 機能ではこの要求を満たすには不十分です。SSO 機能では、認証が必要になると、従来のユーザ クレデンシャル（スタティックなユーザ名とパスワードなど）をクライアントレス Web ベースのリソースに転送するだけであるためです。

たとえば、証明書ベースまたは OTP ベースの認証方式には、ASA が Web ベースのリソースへの SSO アクセスをシームレスに実行するために必要な従来のユーザ名とパスワードは含まれていません。証明書を使用して認証する場合、ASA が Web ベースのリソースへ拡張するためにユーザ名とパスワードは必要ありません。そのため、SSO でサポートされない認証方式になっています。これに対し、OTP にはスタティックなユーザ名が含まれていますが、パスワードはダイナミックであり、VPN セッション中に後で変更されます。一般に、Web ベースのリソースはスタティックなユーザ名とパスワードを受け入れるように設定されるため、OTP も SSO でサポートされない認証方式になっています。

Microsoft の Kerberos Constrained Delegation（KCD）は、ASA のソフトウェア リリース 8.4 で導入された新機能であり、プライベート ネットワーク内の Kerberos で保護された Web アプリケーションへのアクセスを提供します。この利点により、証明書ベースおよび OTP ベースの認証方式を Web アプリケーションにシームレスに拡張できます。したがって、SSO と KCD は独立しながら連携し、多くの組織では、ASA でサポートされるすべての認証方式を使用して、クライアントレス VPN ユーザを認証し、ユーザの認証クレデンシャルを Web アプリケーションにシームレスに拡張できます。

要件

kcd-server コマンドが機能するには、ASA は*ソース ドメイン*（ASA が常駐するドメイン）と*ターゲット*または*リソース ドメイン*（Web サービスが常駐するドメイン）間の信頼関係を確立する必要があります。ASA は、その独自のフォーマットを使用して、サービスにアクセスするリモート アクセス ユーザの代わりに、ソースから宛先ドメインへの認証パスを越えて、必要なチケットを取得します。

このように認証パスを越えることは、クロスレルム認証と呼ばれます。クロスレルム認証の各フェーズで、ASA は特定のドメインのクレデンシャルおよび後続のドメインとの信頼関係に依存しています。

KCD の動作の仕組み

Kerberos は、ネットワーク内のエンティティのデジタル識別情報を検証するために、信頼できる第三者に依存しています。これらのエンティティ（ユーザ、ホスト マシン、ホスト上で実行されるサービスなど）は、プリンシパルと呼ばれ、同じドメイン内に存在している必要があります。秘密キーの代わりに、Kerberos では、サーバに対するクライアントの認証にチケットが使用されます。チケットは秘密キーから導出され、クライアントのアイデンティティ、暗号化されたセッション キー、およびフラグで構成されます。各チケットはキー発行局によって発行され、ライフタイムが設定されます。

Kerberos セキュリティ システムは、エンティティ（ユーザ、コンピュータ、またはアプリケーション）を認証するために使用されるネットワーク認証プロトコルであり、情報の受け手として意図されたデバイスのみが復号化できるようにデータを暗号化することによって、ネットワーク伝送を保護します。クライアントレス SSL VPN ユーザに Kerberos で保護された Web サービスへの SSO アクセスを提供するように KCD を設定できます。このような Web サービスやアプリケーションの例として、Outlook Web Access（OWA）、SharePoint、および Internet Information Server（IIS）があります。

Kerberos プロトコルに対する 2 つの拡張機能として、*プロトコル移行*および*制約付き委任*が実装されました。これらの拡張機能によって、クライアントレスまたは SSL VPN リモート アクセス ユーザは、プライベート ネットワーク内の Kerberos で認証されるアプリケーションにアクセスできます。

*プロトコル移行*では、ユーザ認証レベルでさまざまな認証メカニズムをサポートし、後続のアプリケーション レイヤでセキュリティ機能（相互認証や制約付き委任など）について Kerberos プロトコルに切り替えることによって、柔軟性とセキュリティが強化されます。*制約付き委任*では、ドメイン管理者は、アプリケーションがユーザの代わりを務めることができる範囲を制限することによって、アプリケーション信頼境界を指定して強制適用できます。この柔軟性は、信頼できないサービスによる危険の可能性を減らすことで、アプリケーションのセキュリティ設計を向上させます。

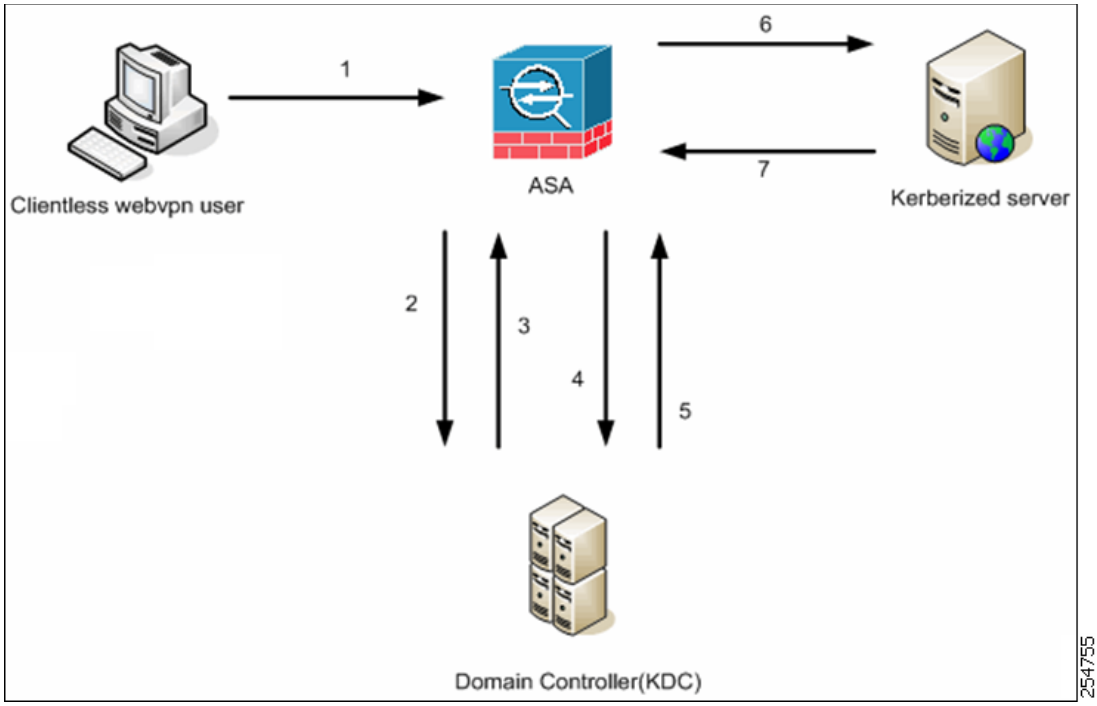
制約付き委任の詳細については、IETF の Web サイト（http://www.ietf.org）にアクセスして、RFC 1510 を参照してください。

KCD の認証フロー

図 12-1 に、委任に対して信頼されたリソースにユーザがクライアントレス ポータルによってアクセスするときに、直接的および間接的に体験するパケットおよびプロセス フローを示します。このプロセスは、次のタスクが完了していることを前提としています。

- ASA 上で設定された KCD
- Windows Active Directory への参加、およびサービスが委任に対して信頼されたことの確認
- Windows Active Directory ドメインのメンバーとして委任された ASA

図 12-1　KCD プロセス



（注）　クライアントレス ユーザ セッションが、ユーザに設定されている認証メカニズムを使用して ASA により認証されます（スマートカード クレデンシャルの場合、ASA によって、デジタル証明書の userPrincipalName を使用して Windows Active Directory に対して LDAP 認可が実行されます）。

1. 認証が成功すると、ユーザは、ASA クライアントレス ポータル ページにログインします。ユーザは、URL をポータル ページに入力するか、ブックマークをクリックして、Web サービスにアクセスします。この Web サービスで認証が必要な場合、サーバは、ASA クレデンシャルの認証確認を行い、サーバでサポートされている認証方式のリストを送信します。

   （注）　クライアントレス SSL VPN の KCD は、すべての認証方式（RADIUS、RSA/SDI、LDAP、デジタル証明書など）に対してサポートされています。次の AAA のサポートに関する表を参照してください。
   http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492

2. 認証確認時の HTTP ヘッダーに基づいて、ASA は、サーバで Kerberos 認証が必要かどうかを決定します （これは SPNEGO メカニズムの一部です）。バックエンド サーバとの接続で、Kerberos 認証が必要な場合、ASA は、ユーザの代わりにそれ自体のために、サービス チケットをキー発行局から要求します。

3. キー発行局は、要求されたチケットを ASA に返します。これらのチケットは ASA に渡されますが、ユーザの認可データが含まれています。ASA は、ユーザがアクセスする特定のサービス用の KDC からのサービス チケットを要求します。

（注）　ステップ 1 ～ 3 では、プロトコル移行が行われます。これらのステップの後、Kerberos 以外の認証プロトコルを使用して ASA に対して認証を行うユーザは、透過的に、Kerberos を使用してキー発行局に対して認証されます。

4. ASA は、ユーザがアクセスする特定のサービス用のキー発行局からのサービス チケットを要求します。
5. キー発行局は、特定のサービスのサービス チケットを ASA に返します。
6. ASA は、サービス チケットを使用して、Web サービスへのアクセスを要求します。
7. Web サーバは、Kerberos サービス チケットを認証して、サービスへのアクセスを付与します。認証が失敗した場合は、適切なエラー メッセージが表示され、確認を求められます。Kerberos 認証が失敗した場合、予期された動作は基本認証にフォールバックします。

Active Directory での Windows サービス アカウントの追加

ASA での KCD 実装にはサービス アカウントが必要です。これはつまり、コンピュータの追加（ドメインへの ASA の追加など）に必要な権限を持った Active Directory ユーザ アカウントです。ここでの例では、Active Directory ユーザ名 JohnDoe は、必要な権限を持ったサービス アカウントを示します。ユーザ権限を Active Directory に実装する方法の詳細については、Microsoft サポートに問い合わせるか、http://microsoft.com を参照してください。

KCD の DNS の設定

この項では、ASA で DNS を設定するために必要な設定手順の概要を示します。KCD を ASA での認証委任方式として使用する場合、ホスト名の解決と、ASA、ドメイン コントローラ（DC）、および委任に対して信頼されたサービス間の通信をイネーブルにするために、DNS が必要です。

ステップ 1　ASDM から、[Configuration] > [Remote Access VPN] > [DNS] に移動し、DNS のセットアップを設定します。

- [DNS Server Group]：DNS サーバの IP アドレス（192.168.0.3 など）を入力します。
- [Domain Name]：DC が属するドメイン名を入力します。

ステップ 2　適切なインターフェイスで DNS ルックアップをイネーブルにします。クライアントレス VPN の配置には、社内ネットワーク（通常は*内部*インターフェイス）を介した DNS ルックアップが必要です。

Active Directory ドメインに参加する ASA の設定

この項では、ASA が Active Directory ドメインの一部として機能できるようにするために必要な設定手順の概要を示します。KCD では、ASA が Active Directory ドメインのメンバーであることが必要です。この設定により、ASA と KCD サーバ間の制約付き委任トランザクションに必要な機能がイネーブルになります。

ステップ 1　ASDM から、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Microsoft KCD Server] に移動します。

ステップ 2　[New] をクリックして制約付き委任用の Kerberos サーバ グループを追加し、次の項目を設定します。

- Server Group Configuration
  - [Server Group Name]：ASA での制約付き委任設定の名前を定義します。MSKCD（デフォルト値）などです。冗長性のために複数のサーバ グループを設定できます。ただし、VPN ユーザの代わりにサービス チケットを要求するために使用する KCD サーバ設定には、割り当てることができるサーバ グループは 1 つのみです。
  - [Reactivation Mode]：目的のモードに対応するオプション ボタンをクリックします（[Depletion] または [Timed]）。[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。[Timed] モードでは、障害が発生したサーバは 30 秒のダウンタイムの後で再アクティブ化されます。[Depletion] がデフォルト設定です。
  - [Dead Time]：再アクティブ化モードとして [Depletion] を選択した場合は、デッド時間を追加する必要があります。10 分がデフォルト設定です。この時間は、グループ内の最後のサーバが非アクティブになってから、すべてのサーバを再度イネーブルにするまでの時間を分単位で表します。
  - [Max Failed Attempts]：応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数を設定します。デフォルトの試行回数は 3 回です。
- Server Configuration
  - [Interface Name]：サーバが常駐するインターフェイスを選択します。一般に、認証サーバの配置は、社内ネットワークに（通常は*内部*インターフェイスを介して）常駐します。
  - [Server Name]：ドメイン コントローラのホスト名を定義します。ServerHostName などです。
  - [Timeout]：サーバからの応答を待機する最大時間（秒単位）を指定します。デフォルトは 10 秒です。
- Kerberos Parameter
  - [Server Port]：88 がデフォルトであり、KCD 用に使用される標準ポートです。
  - [Retry Interval]：必要な再試行間隔を選択します。10 秒がデフォルト設定です。
  - [Realm]：DC のドメイン名をすべて大文字で入力します。ASA での KCD 設定では、レルム値は大文字である必要があります。レルムとは認証ドメインのことです。サービスは、同じレルム内のエンティティからの認証クレデンシャルのみを受け入れることができます。レルムは、ASA が参加するドメイン名と一致している必要があります。

ステップ 3　[OK] をクリックして設定を適用し、リモート アクセス ユーザの代わりにサービス チケットを要求するように Microsoft KCD サーバを設定します。

外部プロキシ サーバの使用法の設定

[Proxies] ペインを使用して、外部プロキシ サーバによって HTTP 要求と HTTPS 要求を処理するように ASA を設定します。これらのサーバは、ユーザとインターネットの仲介役として機能します。すべてのインターネット アクセスがユーザ制御のサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネット アクセスと管理制御が保証されます。

制約事項

HTTP および HTTPS プロキシ サービスでは、PDA への接続をサポートしていません。

ステップ 1　[Use an HTTP Proxy Server] をクリックします。

ステップ 2　IP アドレスまたはホスト名で HTTP プロキシ サーバを識別します。

ステップ 3　外部 HTTP プロキシ サーバのホスト名または IP アドレスを入力します。

ステップ 4　HTTP 要求を受信するポートを入力します。デフォルトのポートは 80 です。

ステップ 5　（オプション）HTTP プロキシ サーバに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。

- * は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。
- **?**は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
- [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。
- [**!***x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。

ステップ 6　（オプション）各 HTTP プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。

ステップ 7　各 HTTP 要求とともにプロキシ サーバに送信されるパスワードを入力します。

ステップ 8　HTTP プロキシ サーバの IP アドレスを指定する方法の代替として、[Specify PAC file URL] を選択して、ブラウザにダウンロードするプロキシ自動コンフィギュレーション ファイルを指定できます。ダウンロードが完了すると、PAC ファイルは JavaScript 機能を使用して各 URL のプロキシを識別します。隣接するフィールドに、**http://** を入力し、プロキシ自動設定ファイルの URL を入力します。**http://** の部分を省略すると、ASA はその URL を無視します。

ステップ 9　HTTPS プロキシ サーバを使用するかどうかを選択します。

ステップ 10　クリックして、IP アドレスまたはホスト名で HTTPS プロキシ サーバを識別します。

ステップ 11　外部 HTTPS プロキシ サーバのホスト名または IP アドレスを入力します。

ステップ 12　HTTPS 要求を受信するポートを入力します。デフォルトのポートは 443 です。

ステップ 13　（オプション）HTTPS プロキシ サーバに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。

- * は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。
- **?**は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。

- [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。
- [!*x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。

ステップ 14　（オプション）各 HTTPS プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、キーワードを入力します。

ステップ 15　各 HTTPS 要求とともにプロキシ サーバに送信されるパスワードを入力します。

SSO サーバ

[SSO Server] ペインでは、Computer Associates SiteMinder SSO サーバまたは Security Assertion Markup Language（SAML）バージョン 1.1 Browser Post Profile SSO サーバに接続するクライアントレス SSL VPN 接続のユーザのシングル サインオン（SSO）を設定または削除できます。クライアントレス SSL VPN でだけ使用できる SSO のサポートにより、ユーザは、ユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。

SSO 設定時に次の方法から選択できます。

- 基本の HTTP または NTLMv1 認証を使用した自動サインオン。
- HTTP Form プロトコル、または Computer Associates eTrust SiteMinder （旧 Netegrity SiteMinder）。
- SAML バージョン 1.1 Browser Post Profile。

制約事項

SAML Browser Artifact プロファイル方式のアサーション交換は、サポートされていません。

次の章では、SiteMinder と SAML Browser Post Profile を使用して SSO を設定する手順について説明します。

- 「SiteMinder と SAML Browser Post Profile の設定」（P.12-8）：基本 HTTP または NTLM 認証で SSO を設定します。
- 「セッションの設定」：HTTP Form プロトコルで SSO を設定します。

SSO のメカニズムは、AAA プロセス（HTTP Form）の一部として開始されるか、AAA サーバ（SiteMinder）または SAML Browser Post Profile サーバへのユーザ認証に成功した直後に開始されます。これらの場合、ASA 上で実行されているクライアントレス SSL VPN サーバは、認証サーバに対してのユーザのプロキシとして機能します。ユーザがログインすると、クライアントレス SSL VPN サーバは、ユーザ名とパスワードを含む SSO 認証要求を HTTPS を使用して認証サーバに送信します。

認証サーバが認証要求を承認すると、SSO 認証クッキーがクライアントレス SSL VPN サーバに返されます。このクッキーは、ユーザの代理として ASA で保持され、ユーザ認証でこのクッキーを使用して、SSO サーバで保護されているドメイン内部の Web サイトの安全を確保します。

SiteMinder と SAML Browser Post Profile の設定

SiteMinder または SAML Browser Post Profile による SSO 認証は AAA から切り離されており、AAA プロセスの完了後に実施されます。ユーザまたはグループが対象の SiteMinder SSO を設定するには、まず AAA サーバ（RADIUS や LDAP など）を設定する必要があります。AAA サーバがユーザを認証した後、クライアントレス SSL VPN サーバは、HTTPS を使用して認証要求を SiteMinder SSO サーバに送信します。

SiteMinder SSO の場合は、ASA の設定を行う以外に、シスコの認証スキームによって CA SiteMinder ポリシー サーバを設定する必要があります。SAML Browser Post Profile の場合は、認証で使用する Web Agent（Protected Resource URL）を設定する必要があります。

サーバ ソフトウェア ベンダーが提供する SAML サーバのマニュアルに従って、SAML サーバを Relying Party モードで設定します。次のフィールドが表示されます。

- [Server Name]：*表示専用*。設定された SSO サーバの名前を表示します。入力できる文字の範囲は、4 ～ 31 文字です。
- [Authentication Type]：*表示専用*。SSO サーバのタイプを表示します。ASA は現在、SiteMinder タイプと SAML Browser Post Profile タイプをサポートしています。
- [URL]：*表示専用*。ASA が SSO 認証要求を行う SSO サーバの URL を表示します。
- [Secret Key]：*表示専用*。SSO サーバとの認証通信の暗号化に使用される秘密キーを表示します。キーは、任意の標準またはシフト式英数字で構成されます。文字の最小数や最大数の制限はありません。
- [Maximum Retries]：*表示専用*。SSO 認証が失敗した場合に ASA がリトライする回数を表示します。リトライの範囲は 1 ～ 5 回で、デフォルトのリトライ数は 3 回です。
- [Request Timeout (seconds)]：*表示専用*。失敗した SSO 認証試行をタイムアウトさせるまでの秒数を表示します。範囲は 1 ～ 30 秒で、デフォルトの秒数は 5 秒です。
- [Add/Edit]：[Add/Edit SSO Server] ダイアログボックスを開きます。
- [Delete]：選択した SSO サーバを削除します。
- [Assign]：SSO サーバを強調表示し、このボタンをクリックして選択したサーバを 1 つ以上の VPN グループ ポリシーまたはユーザ ポリシーに割り当てます。

ステップ 1　アサーティング パーティ（ASA）を表す SAML サーバ パラメータを設定します。

- 宛先コンシューマ（Web Agent）URL（ASA で設定されるアサーション コンシューマ URL と同じ）
- Issuer ID（通常はアプライアンスのホスト名である文字列）
- プロファイル タイプ：Browser Post Profile

ステップ 2　証明書を設定します。

ステップ 3　アサーティング パーティのアサーションには署名が必要なことを指定します。

ステップ 4　SAML サーバがユーザを特定する方法を、次のように選択します。

- Subject Name type が DN
- Subject Name format が uid=<user>

次の作業

「シスコの認証スキームの SiteMinder への追加」を参照してください。

シスコの認証スキームの SiteMinder への追加

SiteMinder による SSO を使用するための ASA の設定に加え、Java プラグインとして提供されている、シスコの認証スキームを使用するようにユーザの CA SiteMinder ポリシー サーバを設定する必要もあります。この項では、手順のすべてではなく、一般的な手順を取り上げます。カスタム認証スキームを追加するための完全な手順については、CA SiteMinder のマニュアルを参照してください。ユーザの SiteMinder ポリシー サーバにシスコの認証スキームを設定するには、次の手順を実行します。

前提条件

SiteMinder ポリシー サーバを設定するには、SiteMinder の経験が必要です。

ステップ 1　SiteMinder Administration ユーティリティを使用して、次の特定の値を使用できるようにカスタム認証スキームを作成します。

- [Library] フィールドに、**smjavaapi** と入力します。
- [Secret] フィールドで、[Add SSO Server] ダイアログの [Secret Key] フィールドで設定したものと同じ秘密キーを入力します。
- [Parameter] フィールドに、**CiscoAuthAPI** と入力します。

ステップ 2　Cisco.com にログインして、http://www.cisco.com/cisco/software/navigator.html から **cisco_vpn_auth.jar** ファイルをダウンロードして、SiteMinder サーバのデフォルトのライブラリ ディレクトリにコピーします。この .jar ファイルは、Cisco ASA CD にも含まれています。

SSO サーバの追加または編集

この SSO 方式では、CA SiteMinder と SAML Browser Post Profile を使用します。また、HTTP Form プロトコルまたは基本 HTML および NTLM 認証を使用して SSO を設定することもできます。基本 HTML または NTLM 認証を使用するように設定する場合は、コマンドライン インターフェイスで **auto sign-on** コマンドを使用します。

ステップ 1　サーバを追加する場合は、新しい SSO の名前を入力します。サーバを編集する場合、このフィールドは表示専用です。選択した SSO サーバの名前が表示されます。

ステップ 2　SSO サーバへの認証要求を暗号化するために使用する秘密キーを入力します。キーに使用する文字には、通常の英数字と、シフト キーを押して入力した英数字を使用できます。文字の最小数や最大数の制限はありません。秘密キーはパスワードに似ており、作成、保存、設定ができます。Cisco Java プラグイン認証スキームを使用して、ASA、SSO サーバ、および SiteMinder ポリシー サーバで設定されます。

ステップ 3　失敗した SSO 認証試行を ASA が再試行する回数を入力します。この回数を超えて失敗すると認証タイムアウトになります。範囲は 1 ～ 5 回で、1 回と 5 回も含まれます。デフォルトは 3 回です。

ステップ 4　失敗した SSO 認証試行をタイムアウトさせるまでの秒数を入力します。範囲は 1 ～ 30 秒で、1 秒と 30 秒も含まれます。デフォルトは 5 秒です。

ステップ 5　[OK] をクリックして設定を適用し、リモート アクセス ユーザの代わりにサービス チケットを要求するように Microsoft KCD サーバを設定します（図 12-1 を参照）。[OK] をクリックすると、Microsoft KCD サーバの設定ウィンドウが表示されます。

次の作業

HTTP Form プロトコルを使用する場合は、「セッションの設定」（P.12-17）を参照してください。

Kerberos サーバ グループの設定

制約付き委任用の Kerberos サーバ グループ MSKCD が、KCD サーバ設定に自動的に適用されます。Kerberos サーバ グループを設定して、[Configuration] > [Remote Access VPN] > [AAA/Local User] > [AAA Server Groups] で管理することもできます。

ステップ 1　[Server Access Credential] セクションで、次の項目を設定します。

- [Username]：サービス アカウント（Active Directory ユーザ名）を定義します。JohnDoe などです。これには、Active Directory ドメインへのコンピュータ アカウントの追加に必要な権限が付与されています。ユーザ名は、特定の管理ユーザには対応せず、単にサービス レベル権限を持つユーザです。このサービス アカウントは、ASA によって、リブートのたびにそれ自体のコンピュータ アカウントを Active Directory ドメインに追加するために使用されます。リモート ユーザの代わりに Kerberos チケットを要求するために、コンピュータ アカウントを個別に設定する必要があります。

（注）　最初の参加には、管理者権限が必要です。ドメイン コントローラのサービス レベル権限を持つユーザはアクセスできません。

- [Password]：ユーザ名に関連付けるパスワードを定義します（Cisco123 など）。パスワードは、特定のパスワードには対応せず、単に Window ドメイン コントローラでデバイスを追加するためのサービス レベル パスワード権限です。

ステップ 2　[Server Group Configuration] セクションで、次の項目を設定します。

- [Reactivation Mode]：使用するモード（[Depletion] または [Timed]）をクリックします。[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。[Timed] モードでは、障害が発生したサーバは 30 秒のダウンタイムの後で再アクティブ化されます。[Depletion] がデフォルト設定です。
- [Dead Time]：再アクティブ化モードとして [Depletion] を選択した場合は、デッド時間を追加する必要があります。この時間は、グループ内の最後のサーバが非アクティブになってから、すべてのサーバを再度イネーブルにするまでの時間を分単位で表します。10 分がデフォルトです。
- [Max Failed Attempts]：応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数を設定します。デフォルトの試行回数は 3 回です。

（注）　[Server Table] セクションでは、前に設定した DC ホスト名 ServerHostName が KCD サーバ設定に自動的に適用されました（図 12-1 を参照）。

ステップ 3　[Apply] をクリックします。

（注）　設定の適用後、ASA によって Active Directory ドメインの参加プロセスが自動的に開始されます。ASA のホスト名が Active Directory Users and Computers の Computers ディレクトリに表示されます。

ASA がドメインに正常に参加したかどうかを確認するには、ASA プロンプトから次のコマンドを実行します。

```
host# show webvpn kcd
Kerberos Realm: WEST.LOCAL
Domain Join: Complete
```

Kerberos で認証されるサービスにアクセスするためのブックマークの設定

Outlook Web Access などの Kerberos で認証されるサービスに ASA クライアントレス ポータルを使用してアクセスするには、ブックマーク リストを設定する必要があります。ブックマーク リストは、リモート アクセス ユーザに関連付けられた VPN セキュリティ ポリシーに基づいて、それらのユーザに割り当てられ、表示されます。

制約事項

Kerberos Constrained Delegation（KCD）を使用するアプリケーションへのブックマークを作成する場合は、[Enable Smart Tunnel] をオンにしないでください。

ステップ 1　ASDM GUI で、[Configuration] > [Remote Access VPN] > [Clientless VPN Access] > [Portal] > [Bookmarks] に移動します。

ステップ 2　[Bookmark List] に、サービス ロケーションを参照するための URL を入力します。

アプリケーション プロファイル カスタマイゼーション フレームワークの設定

クライアントレス SSL アプリケーション プロファイル カスタマイゼーション フレームワーク（APCF）オプションにより、ASA は標準以外のアプリケーションや Web リソースを処理し、クライアントレス SSL VPN 接続で正しく表示できます。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、何（データ）を変換するかを指定するスクリプトがあります。スクリプトは XML 形式で記述され、sed（ストリーム エディタ）の構文を使用して文字列およびテキストを変換します。

ASA では複数の APCF プロファイルを並行して設定および実行できます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。ASA は、設定履歴に基づいて最も古いルールを最初に処理し、次に 2 番目に古いルールを処理します。

APCF プロファイルは、ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存できます。

制約事項

APCF プロファイルは、シスコの担当者のサポートが受けられる場合のみ設定することをお勧めします。

APCF プロファイルの管理

APCF プロファイルは、ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバに保存できます。このペインは、APCF パッケージを追加、編集、および削除する場合と、パッケージを優先順位に応じて並べ替える場合に使用します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Application Helper] の順に進みます。ここでは、次の機能を実行できます。

- [Add/Edit] をクリックして、新しい APCF プロファイルを作成するか、既存の APCF プロファイルを変更します。
  - [Flash file] を選択して、ASA のフラッシュ メモリに保存されている APCF ファイルを指定します。

    次に [Upload] をクリックして、ローカル コンピュータから ASA のフラッシュ ファイル システムに APCF ファイルを取得するか、[Browse] をクリックしてフラッシュ メモリに既存する APCF を選択します。
  - [URL] を選択して、HTTP、HTTPS、FTP、または TFTP サーバから APCF ファイルを取得します。
- [Delete] をクリックして、既存の APCF プロファイルを削除します。確認の画面は表示されず、やり直しもできません。
- [Move Up] または [Move Down] をクリックして、リスト内の APCF プロファイルの順序を入れ替えます。順序は、使用される APCF プロファイルを決定します。

ステップ 2　リストに変更が加えられていない場合は、[Refresh] をクリックします。

APCF パッケージのアップロード

ステップ 1　コンピュータ上にある APCF ファイルへのパスが表示されます。[Browse Local] をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。

ステップ 2　APCF ファイルを見つけて、コンピュータに転送するように選択するにはクリックします。[Select File Path] ダイアログボックスに、自分のローカル コンピュータで最後にアクセスしたフォルダの内容が表示されます。APCF ファイルに移動して選択し、[Open] をクリックします。ASDM が [Local File Path] フィールドにファイルのパスを挿入します。

ステップ 3　APCF ファイルをアップロードする ASA 上のパスが [Flash File System Path] に表示されます。[Browse Flash] をクリックして、APCF ファイルをアップロードする ASA 上の場所を特定します。[Browse Flash] ダイアログボックスに、フラッシュ メモリの内容が表示されます。

ステップ 4　ローカル コンピュータで選択した APCF ファイルのファイル名が表示されます。混乱を防ぐために、この名前を使用することをお勧めします。このファイルの名前が正しく表示されていることを確認し、[OK] をクリックします。[Browse Flash] ダイアログボックスが閉じます。ASDM が [Flash File System Path] フィールドにアップロード先のファイル パスを挿入します。

ステップ 5　自分のコンピュータの APCF ファイルの場所と、APCF ファイルを ASA にダウンロードする場所を特定したら、[Upload File] をクリックします。

ステップ 6　[Status] ウィンドウが表示され、ファイル転送中は開いたままの状態を維持します。転送が終わり、[Information] ウィンドウに「File is uploaded to flash successfully.」というメッセージが表示されたら、[OK] をクリックします。[Upload Image] ダイアログ ウィンドウから、[Local File Path] フィールドと [Flash File System Path] フィールドの内容が削除されます。これは、別のファイルをアップロードできることを表します。別のファイルをアップロードするには、上記の手順を繰り返します。それ以外の場合は、[Close] をクリックします。

ステップ 7　[Upload Image] ダイアログ ウィンドウを閉じます。APCF ファイルをフラッシュ メモリにアップロードした後、またはアップロードしない場合に、[Close] をクリックします。アップロードする場合には、[APCF] ウィンドウの [APCF File Location] フィールドにファイル名が表示されます。アップロードしない場合には、「Are you sure you want to close the dialog without uploading the file?」と尋ねる [Close Message] ダイアログボックスが表示されます。ファイルをアップロードしない場合は、[OK] をクリックします。[Close Message] ダイアログボックスと [Upload Image] ダイアログボックスが閉じられ、APCF [Add/Edit] ペインが表示されます。この処理が実行されない場合は、[Close Message] ダイアログボックスの [Cancel] をクリックします。ダイアログボックスが閉じられ、フィールドの値がそのままの状態で [Upload Image] ダイアログボックスが再度表示されます。[Upload File] をクリックします。

APCF パケットの管理

ステップ 1　クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。

```
webvpn
```

ステップ 2　ASA 上にロードする APCF プロファイルを特定および検索します。

この例では、フラッシュ メモリに保存されている apcf1.xml という名前の APCF プロファイルをイネーブルにする方法と、ポート番号 1440、パスが /apcf の myserver という名前の HTTPS サーバにある APCF プロファイル apcf2.xml をイネーブルにする方法を示します。

```
apcf
```

例：

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml

hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
```

ステップ 1　次のコマンドを使用して、APCF パケットを追加、編集、および削除し、パケットを優先順位に応じて並べ替えます。

- [APCF File Location]：APCF パッケージの場所についての情報を表示します。ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバのいずれかです。
- [Add/Edit]：新規または既存の APCF プロファイルを追加または編集します。

- [Delete]：既存の APCF プロファイルを削除します。確認されず、やり直しもできません。
- [Move Up]：リスト内の APCF プロファイルを再配置します。リストにより、ASA が APCF プロファイルを使用するときの順序が決まります。

ステップ 2　[Flash File] をクリックして、ASA のフラッシュ メモリに保存されている APCF ファイルを指定します。

ステップ 3　フラッシュ メモリに保存されている APCF ファイルのパスを入力します。パスをすでに追加している場合は、そのパスを特定するために参照した後、フラッシュ メモリに格納された APCF ファイルにリダイレクトします。

ステップ 4　[Browse Flash] をクリックして、フラッシュ メモリを参照し、APCF ファイルを指定します。[Browse Flash Dialog] ペインが表示されます。[Folders] および [Files] 列を使用して APCF ファイルを指定します。APCF ファイルを選択して、[OK] をクリックします。ファイルへのパスが [Path] フィールドに表示されます。

（注）　最近ダウンロードした APCF ファイルの名前が表示されない場合には、[Refresh] をクリックします。

- [Upload] : APCF ファイルをローカル コンピュータから ASA のフラッシュ ファイル システムにアップロードします。[Upload APCF Package] ペインが表示されます。
- [URL] : HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存されている APCF ファイルを使用する場合にクリックします。
- [ftp, http, https, and tftp (unlabeled)]：サーバ タイプを特定します。
- [URL (unlabeled)]：FTP、HTTP、HTTPS、または TFTP サーバへのパスを入力します。

APCF 構文

APCF プロファイルは、XML フォーマットおよび sed スクリプトの構文を使用します。表 12-1 に、この場合に使用する XML タグを示します。

ガイドライン

APCF プロファイルの使い方を誤ると、パフォーマンスが低下したり、好ましくない表現のコンテンツになる場合があります。シスコのエンジニアリング部では、ほとんどの場合、APCF プロファイルを提供することで特定アプリケーションの表現上の問題を解決しています。

表 12-1　APCF XML タグ

タグ	使用目的
<APCF>...</APCF>	すべての APCF XML ファイルを開くための必須のルート要素。
<version>1.0</version>	APCF の実装バージョンを指定する必須のタグ。現在のバージョンは 1.0 だけです。
<application>...</application>	XML 記述の本文を囲む必須タグ。
<id> text </id>	この特定の APCF 機能を記述する必須タグ。

表 12-1　APCF XML タグ（続き）

タグ	使用目的
<apcf-entities>...</apcf-entities>	単一または複数の APCF エンティティを囲む必須タグ。
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	これらのタグのうちの 1 つが、コンテンツの種類または APCF 処理が実施される段階を指定します。
<conditions>… </conditions>	処理前および処理後の子要素タグで、次の処理基準を指定します。 • http-version（1.1、1.0、0.9 など） • http-method（get、put、post、webdav） • http-scheme（"http/"、"https/"、その他） • （"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?"）を含む server-regexp 正規表現 • （"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"）を含む server-fnmatch 正規表現 • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • 条件タグのうち 2 つ以上が存在する場合は、ASA はすべてのタグに対して論理 AND を実行します。
<action> … </action>	指定した条件で 1 つ以上のアクションをコンテンツでラップします。これらのアクションを定義するには、次のタグを使用できます（下記参照）。 • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

表 12-1　APCF XML タグ（続き）

タグ	使用目的
<do>…</do>	次のいずれかのアクションの定義に使用されるアクション タグの子要素です。 • <no-rewrite/>：リモート サーバから受信したコンテンツを上書きしません。 • <no-toolbar/>：ツールバーを挿入しません。 • <no-gzip/>：コンテンツを圧縮しません。 • <force-cache/>:元のキャッシュ命令を維持します。 • <force-no-cache/>：オブジェクトをキャッシュできないようにします。 • < downgrade-http-version-on-backend>：リモート サーバに要求を送信するときに HTTP/1.0 を使用します。
<sed-script> TEXT </sed-script>	テキストベースのオブジェクトのコンテンツの変更に使用されるアクション タグの子要素です。TEXT は有効な Sed スクリプトである必要があります。<sed-script> は、これより前に定義された <conditions> タグに適用されます。
<rewrite-header></rewrite-header>	アクション タグの子要素です。<header> の子要素タグで指定された HTTP ヘッダーの値を変更します（以下を参照してください）。
<add-header></add-header>	<header> の子要素タグで指定された新しい HTTP ヘッダーの追加に使用されるアクション タグの子要素です（以下を参照してください）。
<delete-header></delete-header>	<header> の子要素タグで指定された特定の HTTP ヘッダーの削除に使用されるアクション タグの子要素です（以下を参照してください）。
<header></header>	上書き、追加、または削除される HTTP ヘッダー名を指定します。たとえば、次のタグは Connection という名前の HTTP ヘッダーの値を変更します。 <rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header>

APCF の設定例

例：

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.example.com</server-fnmatch>
```

```
          </conditions>
            <action>
              <do><no-gzip/></do>
            </action>
       </process-request-header>
  </apcf-entities>
</application>
</APCF>
```

例：

```
<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
           <rewrite-header>
                <header>Content-Type</header>
                <value>text/html</value>
           </rewrite-header>
         </action>
      </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

セッションの設定

[Clientless SSL VPN Add/Edit Internal Group Policy] > [More Options] > [Session Settings] ウィンドウでは、クライアントレス SSL VPN のセッションからセッションの間にパーソナライズされたユーザ情報を指定できます。デフォルトにより、各グループ ポリシーはデフォルトのグループ ポリシーから設定を継承します。このウィンドウを使用して、デフォルト グループ ポリシーのパーソナライズされたクライアントレス SSL VPN ユーザ情報、およびこれらの設定値を区別するグループ ポリシーすべてを指定します。

ステップ 1　[none] をクリックするか、または [User Storage Location] ドロップダウン メニューからファイル サーバ プロトコル（smb または ftp）をクリックします。シスコでは、ユーザ ストレージに CIFS を使用することを推奨します。ユーザ名/パスワードまたはポート番号を使用せずに CIFS を設定できます。[CIFS] を選択する場合は、次の構文を入力します。

```
cifs//cifs-share/user/data
```

[smb] または [ftp] を選択する場合は、次の構文を使用して、隣のテキスト フィールドにファイル システムの宛先を入力します。

```
username:password@host:port-number/path
```

次に例を示します。

mike:mysecret@ftpserver3:2323/public

（注）　このコンフィギュレーションには、ユーザ名、パスワード、および事前共有キーが示されていますが、ASA は、内部アルゴリズムを使用して暗号化された形式でデータを保存し、そのデータを保護します。

ステップ 2　必要な場合は、保管場所へユーザがアクセスできるようにするためにセキュリティ アプライアンスが渡す文字列を入力します。

ステップ 3　[Storage Objects] ドロップダウン メニューから次のいずれかのオプションを選択して、ユーザとの関連でサーバが使用するオブジェクトを指定します。ASA は、これらのオブジェクトを保存してクライアントレス SSL VPN 接続をサポートします。

- cookies,credentials
- cookies
- credentials

ステップ 4　セッションをタイムアウトするときのトランザクション サイズの限界値を KB 単位で入力します。この属性は、1 つのトランザクションにだけ適用されます。この値よりも大きなトランザクションだけが、セッションの期限切れクロックをリセットします。

エンコーディング

*文字エンコーディング*は「文字コード」や「文字セット」とも呼ばれ、raw データ（0 や 1 など）を文字と組み合わせ、データを表します。使用する文字エンコード方式は、言語によって決まります。単一の方式を使う言語もあれば、使わない言語もあります。通常は、地域によってブラウザで使用されるデフォルトのコード方式が決まりますが、リモート ユーザが変更することもできます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。

エンコード属性によりポータル ページで使用される文字コード方式の値を指定することで、ユーザがブラウザを使用している地域や、ブラウザに対する何らかの変更に関係なく、ページが正しく表示されるようにできます。

デフォルトでは、ASA は「Global Encoding Type」を Common Internet File System（共通インターネット ファイル システム）サーバからのページに適用します。CIFS サーバと適切な文字エンコーディングとのマッピングを、[Global Encoding Type] 属性によってグローバルに、そしてテーブルに示されているファイル エンコーディング例外を使用して個別に行うことにより、ファイル名やディレクトリ パス、およびページの適切なレンダリングが問題となる場合に、CIFS ページが正確に処理および表示できるようにします。

文字エンコーディングの表示または指定

エンコーディングを使用すると、クライアントレス SSL VPN ポータル ページの文字エンコーディングを表示または指定できます。

ステップ 1　[Global Encoding Type] によって、表に記載されている CIFS サーバからの文字エンコーディングを除いて、すべてのクライアントレス SSL VPN ポータル ページが継承する文字エンコーディングが決まります。文字列を入力するか、ドロップダウン リストから選択肢を 1 つ選択します。リストには、最も一般的な次の値だけが表示されます。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis
- unicode
- windows-1252
- none

（注）　[none] をクリックするか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

最大 40 文字から成り、http://www.iana.org/assignments/character-sets で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。ASA の設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。

ステップ 2　エンコーディング要件が「Global Encoding Type」属性設定とは異なる CIFS サーバの名前または IP アドレスを入力します。ASA では、指定した大文字と小文字の区別が保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。

ステップ 3　CIFS サーバがクライアントレス SSL VPN ポータル ページに対して指定する必要のある文字エンコーディングを選択します。文字列を入力するか、ドロップダウン リストから選択します。リストには、最も一般的な次の値だけが登録されています。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

（注）　日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do Not Specify] をクリックして、このフォント ファミリを削除します。

- unicode
- windows-1252
- none

[none] をクリックするか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

最大 40 文字から成り、http://www.iana.org/assignments/character-sets で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。ASA の設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。

頻繁に再利用されるオブジェクトの格納

キャッシュにより、クライアントレス SSL VPN のパフォーマンスを強化します。頻繁に再利用されるオブジェクトをシステム キャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。キャッシュを使用することでトラフィック量が減り、結果として多くのアプリケーションがより効率的に実行されます。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Content Cache] の順に選択します。

ステップ 2　[Enable Cache] がオフの場合は、オンにします。

ステップ 3　キャッシング条件を定義します。

- [Maximum Object Size]：ASA がキャッシュできるドキュメントの最大サイズを KB 単位で入力します。ASA が、オブジェクトの元の（書き換えまたは圧縮されていない）コンテンツの長さを測定します。範囲は 0 ～ 10,000 KB で、デフォルトは 1,000 KB です。
- [Minimum Object Size]：ASA がキャッシュできるドキュメントの最小サイズを KB 単位で入力します。ASA が、オブジェクトの元の（書き換えまたは圧縮されていない）コンテンツの長さを測定します。範囲は 0 ～ 10,000 KB で、デフォルトは 0 KB です。

（注）　[Maximum Object Size] は、[Minimum Object Size] よりも大きい値にする必要があります。

- [Expiration Time]：0 ～ 900 の整数を入力して、オブジェクトを再検証しないでキャッシュする分数を設定します。デフォルトは 1 分です。
- [LM Factor]：1 ～ 100 の整数を入力します。デフォルトは 20 です。

  LM 因数は、最終変更タイムスタンプだけを持つオブジェクトをキャッシュするためのポリシーを設定します。これによって、サーバ設定の変更値を持たないオブジェクトが再検証されます。ASA は、オブジェクトが変更された後、およびオブジェクトが期限切れの時刻を呼び出した後の経過時間を推定します。推定された期限切れ時刻は、最終変更後の経過時間と LM 因数の積に一致します。LM 因数を 0 に設定すると、ただちに再検証が実行され、100 に設定すると、再検証までの許容最長時間になります。

  期限切れ時刻は、ASA が、最終変更タイムスタンプがなく、サーバ設定の期限切れ時刻も明示されていないオブジェクトをキャッシュする時間の長さを設定します。

- [Cache static content]：たとえば PDF ファイルやイメージなど、リライトされることのないすべてのコンテンツをキャッシュします。
- [Restore Cache Default]：すべてのキャッシュ パラメータをデフォルト値に戻します。

Content Rewrite

[Content Rewrite] ペインには、コンテンツのリライトがイネーブルになっているか、またはオフに切り替わっているすべてのアプリケーションが一覧表示されます。

クライアントレス SSL VPN では、コンテンツ変換およびリライト エンジンによって、JavaScript、VBScript、Java、マルチバイト文字などの高度な要素からプロキシ HTTP へのトラフィックまでを含む、アプリケーション トラフィックを処理します。このようなトラフィックでは、ユーザがアプリケーションにアクセスするのに SSL VPN デバイス内部からアプリケーションを使用しているか、SSL VPN デバイスに依存せずに使用しているかによって、セマンティックやアクセス コントロールのルールが異なる場合があります。

デフォルトでは、セキュリティ アプライアンスはすべてのクライアントレス トラフィックをリライト、または変換します。一部のアプリケーション（公開 Web サイトなど）や Web リソースによっては、ASA を通過しない設定が求められる場合があります。このため、ASA では、特定のサイトやアプリケーションを ASA を通過せずにブラウズできるリライト ルールを作成できます。これは、VPN 接続におけるスプリット トンネリングに似ています。

（注）　これらの機能強化は、ASA 9.0 の Content Rewriter に行われました。

- コンテンツ リライトは、HTML5 に対するサポートを追加しました。
- クライアントレス SSL VPN リライタ エンジンの品質と有効性が大きく向上しました。その結果、クライアントレス SSL VPN ユーザのエンドユーザ エクスペリエンスも向上が期待できます。

リライト ルールの作成

リライト ルールは複数作成できます。セキュリティ アプライアンスはリライト ルールを順序番号に従って検索するため、ルールの番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

[Content Rewrite] テーブルには、次のカラムがあります。

- [Rule Number]：リスト内でのルールの位置を示す整数を表示します。
- [Rule Name]：ルールが適用されるアプリケーションの名前を付けます。
- [Rewrite Enabled]：コンテンツのリライトをイネーブルかオフで表示します。
- [Resource Mask]：リソース マスクを表示します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Content Rewrite] の順に進みます。

ステップ 2　[Add] または [Edit] をクリックして、コンテンツ リライト ルールを作成または更新します。

ステップ 3　このルールをイネーブルにするには、[Enable content rewrite] をオンにします。

ステップ 4　このルールの番号を入力します。この番号は、リストの他のルールに相対的に、そのルールの優先順位を示します。番号がないルールはリストの最後に配置されます。有効な範囲は 1 ～ 65534 です。

ステップ 5　（オプション）ルールについて説明する英数字を指定します。最大 128 文字です。

ステップ 6　ルールを適用するアプリケーションやリソースに対応する文字列を入力します。文字列の長さは最大で 300 文字です。次のいずれかのワイルドカードを使用できますが、少なくとも 1 つの英数字を指定する必要があります。

* : すべてに一致します。ASDM では、* または *.* で構成されるマスクは受け付けません。

? : 単一文字と一致します。

[!seq] : シーケンスにない任意の文字と一致します。

[seq] : シーケンスにある任意の文字と一致します。

コンテンツ リライト ルールの設定例

表 12-2　コンテンツ リライト ルール

機能	コンテンツ リライトのイネーブル	ルール番号	ルール名	リソース マスク
youtube.com での HTTP URL のリライタをオフに切り替える	オフ	1	no-rewrite-youtube	*.youtube.com/*
上記のルールに一致しないすべての HTTP URL のリライタをイネーブルにする	オン	65,535	rewrite-all	*

クライアントレス SSL VPN を介した電子メールの使用

Web 電子メールの設定：MS Outlook Web App

ASA は、Microsoft Outlook Web App to Exchange Server 2010 および Microsoft Outlook Web Access to Exchange Server 2007、2003、および 2000 をサポートしています。

ステップ 1　アドレス フィールドに電子メール サービスの URL を入力するか、クライアントレス SSL VPN セッションでの関連するブックマークをクリックします。

ステップ 2　プロンプトが表示されたら、電子メール サーバのユーザ名を *domain\username* 形式で入力します。

ステップ 3　電子メール パスワードを入力します。

ブックマークの設定

[Bookmarks] パネルでは、ブックマーク リストを追加、編集、削除、インポート、およびエクスポートできます。

[Bookmarks] パネルを使用して、クライアントレス SSL VPN でアクセスするための、サーバおよび URL のリストを設定します。ブックマーク リストのコンフィギュレーションに続いて、そのリストを 1 つ以上のポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に割り当てることができます。各ポリシーのブックマーク リストは 1 つのみです。リスト名は、各 DAP の [URL Lists] タブのドロップダウン リストに表示されます。

一部の Web ページでの自動サインオンに、マクロ置換を含むブックマークを使用できるようになりました。以前の POST プラグイン アプローチは、管理者がサインオン マクロを含む POST ブックマークを指定し、POST 要求のポストの前にロードするキックオフ ページを受信できるようにするために作成されました。この POST プラグイン アプローチでは、クッキーまたはその他のヘッダー項目の存在を必要とする要求は排除されました。現在は、管理者は事前ロード ページおよび URL を決定し、これによってポスト ログイン要求の送信場所が指定されます。事前ロード ページによって、エンドポイント ブラウザは、クレデンシャルを含む POST 要求を使用するのではなく、Web サーバまたは Web アプリケーションに送信される特定の情報を取得できます。

既存のブックマーク リストが表示されます。ブックマーク リストを追加、編集、削除、インポート、またはエクスポートできます。アクセス用のサーバおよび URL のリストを設定し、指定した URL リスト内の項目を配列することができます。

ガイドライン

ブックマークを設定することでは、ユーザが不正なサイトや会社のアクセプタブル ユース ポリシーに違反するサイトにアクセスすることを防ぐことはできません。ブックマーク リストをグループ ポリシー、ダイナミック アクセス ポリシー、またはその両方に割り当てる以外に、Web ACL をこれらのポリシーに割り当てて、トラフィック フローへのアクセスを制御します。これらのポリシー上の URL エントリをオフに切り替えて、ユーザがアクセスできるページについて混乱しないようにします。

ステップ 1　追加するリストの名前を指定するか、修正または削除するリストの名前を選択します。

ブックマークのタイトルおよび実際の関連付けられた URL が表示されます。

ステップ 2　（オプション）[Add] をクリックして、新しいサーバまたは URL を設定します。次のいずれかを追加できます。

- GET または Post メソッドによる URL のブックマークの追加
- 定義済みアプリケーション テンプレートに対する URL の追加
- 自動サインオン アプリケーションへのブックマークの追加

ステップ 3　（オプション）[Edit] をクリックして、サーバ、URL、または表示名を変更します。

ステップ 4　（オプション）[Delete] をクリックして、選択した項目を URL リストから削除します。確認の画面は表示されず、やり直しもできません。

ステップ 5　（オプション）ファイルのインポート元またはエクスポート元の場所を選択します。

- [Local computer]：ローカル PC に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Flash file system]：ASA に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Remote server]：ASA からアクセス可能なリモート サーバに常駐するファイルをインポートする場合にクリックします。
- [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- [Browse Local Files/Browse Flash...]：ファイルのパスを参照します。

ステップ 6　（オプション）ブックマークを強調表示し、[Assign] をクリックして、選択したブックマークを 1 つ以上のグループ ポリシー、ダイナミック アクセス ポリシー、または LOCAL ユーザに割り当てます。

ステップ 7　（オプション）[Move Up] または [Move Down] オプションを使用して、選択した項目の位置を URL リスト内で変更します。

ステップ 8　[OK] をクリックします。

次の作業

クライアントレス SSL VPN セキュリティ対策について確認してください。

GET または Post メソッドによる URL のブックマークの追加

[Add Bookmark Entry] ダイアログボックスでは、URL リストのリンクまたはブックマークを作成できます。

前提条件

ネットワークの共有フォルダにアクセスするには、\\server\share\subfolder\<*personal folder*> 形式を使用します。<*personal folder*> の上のすべてのポイントに対するリスト権限がユーザに必要です。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] の順に進み、[Add] ボタンをクリックします。

ステップ 2　[URL with GET or POST Method] を選択して、ブックマークの作成に使用します。

ステップ 3　ポータルに表示されるこのブックマークの名前を入力します。

ステップ 4　[URL] ドロップダウン メニューを使用して、URL タイプ（http、https、cifs、または ftp）を選択します。[URL] ドロップダウンは、標準の URL タイプ、インストールしたすべてのプラグインのタイプを示します。

ステップ 5　このブックマーク（URL）の DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符（/?）を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。

server`/?`*Parameter*`=`*Value*`&`*Parameter*`=`*Value*

次に例を示します。

host`/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768`

プラグインによって、入力できるオプションのパラメータ/値ペアが決まります。

プラグインに対して、シングル サインオン サポートを提供するには、パラメータ/値ペア **csco_sso=1** を使用します。次に例を示します。

host`/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768`

ステップ 6　（オプション）事前ロード URL を入力します。事前ロード URL を入力するときに、待機時間も入力できます。待機時間は、実際の POST URL に転送されるまでに、ページのロードに使用できる時間です。

ステップ 7　サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。

ステップ 8　[Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。

ステップ 9　[Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。

ステップ 10　クリックしてブックマークを新しいウィンドウで開きます。このウィンドウでは、スマート トンネル機能を使用し、ASA を経由して宛先サーバとのデータの送受信を行います。すべてのブラウザ トラフィックは、SSL VPN トンネルで安全に送受信されます。このオプションでは、ブラウザベースのアプリケーションにスマート トンネルのサポートを提供します。一方で、[Smart Tunnels]（[Clientless SSL VPN] > [Portal] メニューにもあり）では、非ブラウザベースのアプリケーションもスマート トンネル リストに追加し、それをグループ ポリシーとユーザ名に割り当てられます。

ステップ 11　[Allow the Users to Bookmark the Link] をオンにして、クライアントレス SSL VPN ユーザが、ブラウザの [Bookmarks] または [Favorites] オプションを使用できるようにします。選択を解除すると、これらのオプションを使用できません。このオプションをオフにすると、クライアントレス SSL VPN ポータルの [Home] セクションにブックマークは表示されません。

ステップ 12　（オプション）[Advanced Options] を選択して、ブックマークの特徴の詳細を設定します。

- [URL Method]：単純なデータ取得の場合には [Get] を選択します。データの保存または更新、製品の注文、電子メールの送信など、データを処理することによってデータに変更が加えられる可能性がある場合には、[Post] を選択します。
- [Post Parameters]：Post URL 方式の詳細を設定します。

定義済みアプリケーション テンプレートに対する URL の追加

このオプションは、事前に定義された ASDM テンプレートを選択しているユーザのブックマークの作成を簡略化します。ASDM テンプレートには、特定の明確に定義されたアプリケーションに対する事前に入力された必要な値が含まれます。

前提条件

定義済みアプリケーションのテンプレートは、次のアプリケーションで現在使用できます。

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010

ステップ 1　ユーザに対して表示するブックマークの名前を入力します。

ステップ 2　サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。

ステップ 3　[Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。

ステップ 4　[Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。

ステップ 5　（オプション）[Place This Bookmark on the VPN Home Page] チェックボックスをオンにします。

ステップ 6　[Select Auto Sign-on Application] リストで、必要なアプリケーションをクリックします。使用可能なアプリケーションは次のとおりです。

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010

ステップ 7　ログイン ページの前にロードされたページの URL を入力します。このページには、ログイン画面に進むためのユーザ インタラクションが必要になります。URL には、任意の記号の番号を置き換える * を入力できます（たとえば、http*://www.example.com/test）。

ステップ 8　[Pre-login Page Control ID] を入力します。これは、ログイン ページに進む前に事前ログイン ページの URL でクリック イベントを取得する制御/タグの ID です。

ステップ 9　[Application Parameters] を入力します。アプリケーションに応じて、次の内容が含まれる可能性があります。

- [Protocol]：HTTP または HTTPS。
- [hostname]：たとえば、`www.cisco.com` などです。
- [Port Number]：アプリケーションで使用されるポート。
- [URL Path Appendix]：たとえば、`/Citrix/XenApp` などです。通常これは、自動入力されます。
- [Domain]：接続するドメイン。
- [User Name]：ユーザ名として使用する SSL VPN 変数。[Select Variable] をクリックして、異なる変数を選択します。
- [Password]：パスワードとして使用する SSL VPN 変数。[Select Variable] をクリックして、異なる変数を選択します。

ステップ 10　（オプション）[Preview] をクリックして、テンプレートの出力を表示します。[Edit] をクリックして、テンプレートを変更できます。

ステップ 11　[OK] をクリックして、変更を行います。または、[Cancel] をクリックして変更を破棄します。

自動サインオン アプリケーションへのブックマークの追加

このオプションでは、複雑な自動サインオン アプリケーションのブックマークを作成できます。

前提条件

自動サインオン アプリケーションの設定には、2 つの手順が必要になります。

1. 基本的な初期データがあり、POST パラメータがないブックマークを定義します。ブックマークを保存および割り当てて、グループまたはユーザ ポリシーで使用します。
2. ブックマークを再度編集します。特定のキャプチャ機能を使用して、SSL VPN パラメータをキャプチャし、ブックマークで編集します。

ステップ 1　ユーザに対して表示するブックマークの名前を入力します。

ステップ 2　[URL] ドロップダウン メニューを使用して、URL タイプ（http、https、cifs、または ftp）を選択します。インポートされたすべてのプラグインの URL タイプが、このメニューに表示されます。ポータル ページにリンクとしてプラグインを表示するには、プラグインの URL タイプを選択します。

ステップ 3　ブックマークの DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符（/?）を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。

server`/?`*Parameter*`=`*Value*`&`*Parameter*`=`*Value*

次に例を示します。

host`/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768`

プラグインによって、入力できるオプションのパラメータ/値ペアが決まります。

プラグインに対して、シングル サインオン サポートを提供するには、パラメータ/値ペア **csco_sso=1** を使用します。次に例を示します。

host`/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768`

ステップ 4　サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。

ステップ 5　[Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。

ステップ 6　[Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。

ステップ 7　（オプション）[Place This Bookmark on the VPN Home Page] チェックボックスをオンにします。

ステップ 8　[Login Page URL] を入力します。入力する URL には、ワイルドカードを使用できます。たとえば、`http*://www.example.com/myurl*` と入力します。

ステップ 9　[Landing Page URL] を入力します。ASA では、アプリケーションへの正常なログインを検出するために、ランディング ページを設定する必要があります。

ステップ 10　（オプション）[Post Script] を入力します。Microsoft Outlook Web Access などの一部の Web アプリケーションは、JavaScript を実行して、ログイン フォームを送信する前に、要求パラメータを変更する場合があります。[Post Script] フィールドでは、このようなアプリケーションの JavaScript を入力できます。

ステップ 11　必要な [Form Parameters] を追加します。それぞれの必要な SSL VPN 変数では、[Add] をクリックして、[Name] を入力して、リストから変数を選択します。[Edit] をクリックしてパラメータを変更し、[Delete] をクリックして削除することができます。

ステップ 12　ログイン ページの前にロードされたページの URL を入力します。このページには、ログイン画面に進むためのユーザ インタラクションが必要になります。URL には、任意の記号の番号を置き換える * を入力できます（たとえば、http*://www.example.com/test）。

ステップ 13　[Pre-login Page Control ID] を入力します。これは、ログイン ページに進む前に事前ログイン ページの URL でクリック イベントを取得する制御/タグの ID です。

ステップ 14　[OK] をクリックして、変更を行います。または、[Cancel] をクリックして変更を破棄します。

ブックマークを編集する場合、HTML Parameter Capture 機能を使用して、VPN 自動サインオン パラメータをキャプチャできます。ブックマークは保存され、グループ ポリシーまたはユーザにまず割り当てられる必要があります。

[SSL VPN Username] を入力してから、[Start Capture] をクリックします。次に、Web ブラウザを使用して、VPN セッションを開始して、イントラネットのページに進みます。プロセスを完了するには、[Stop Capture] をクリックします。パラメータが編集できるようになり、ブックマークに挿入されます。

ブックマーク リストのインポートおよびエクスポート

すでに設定済みのブックマーク リストは、インポートまたはエクスポートできます。使用準備ができているリストをインポートします。リストをエクスポートして修正または編集してから、再インポートすることもできます。

ステップ 1　ブックマーク リストを名前で指定します。最大 64 文字で、スペースは使用できません。

ステップ 2　リスト ファイルをインポートする、またはエクスポートするための方法を選択します。

- [Local computer]：ローカル PC に常駐するファイルをインポートする場合に選択します。
- [Flash file system]：ASA に常駐するファイルをエクスポートする場合に選択します。
- [Remote server]：ASA からアクセス可能なリモート サーバに常駐する URL リスト ファイルをインポートする場合にクリックします。
- [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- [Browse Local Files/Browse Flash]：ファイルのパスを参照します。
- [Import/Export Now]：リスト ファイルをインポートまたはエクスポートします。

[Import and Export GUI Customization Objects (Web Contents)]

このダイアログボックスでは、Web コンテンツ オブジェクトをインポートおよびエクスポートできます。Web コンテンツ オブジェクトの名前とファイル タイプが表示されます。

Web コンテンツには、全体的に設定されたホーム ページから、エンド ユーザ ポータルをカスタマイズするときに使用するアイコンやイメージまで、さまざまな種類があります。設定済みの Web コンテンツは、インポートまたはエクスポートできます。使用準備ができている Web コンテンツをインポートします。Web コンテンツをエクスポートして修正または編集してから、再インポートすることもできます。

ステップ 1　ファイルのインポート元またはエクスポート元の場所を選択します。

- [Local computer]：ローカル PC に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Flash file system]：ASA に常駐するファイルをインポートまたはエクスポートする場合にクリックします。

- [Remote server]：ASA からアクセス可能なリモート サーバに常駐するファイルをインポートする場合にクリックします。
- [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- [Browse Local Files.../Browse Flash...]：ファイルのパスを参照します。

ステップ 2　コンテンツへのアクセスに認証が必要かどうかを決定します。

パスのプレフィックスは、認証を要求するかどうかに応じて異なります。ASA は、認証が必要なオブジェクトの場合には /+CSCOE+/ を使用し、認証が不要なオブジェクトの場合には /+CSCOU+/ を使用します。ASA はポータル ページにだけ /+CSCOE+/ オブジェクトを表示するのに対し、/+CSCOU+/ オブジェクトは、ログイン ページまたはポータル ページのどちらかで表示または使用可能です。

ステップ 3　クリックして、ファイルをインポートまたはエクスポートします。

[Add and Edit Post Parameters]

このペインでは、ブックマーク エントリと URL リストのポスト パラメータを設定します。

クライアントレス SSL VPN 変数により、URL およびフォームベースの HTTP post 操作で置換が実行できます。これらの変数はマクロとも呼ばれ、ユーザ ID とパスワード、またはその他の入力パラメータを含む、パーソナル リソースへのユーザ アクセスを設定できます。このようなリソースの例には、ブックマーク エントリ、URL リスト、およびファイル共有などがあります。

ステップ 1　パラメータの名前と値を、対応する HTML フォームのとおりに指定します。たとえば、

`<input name="param_name" value="param_value">` **です。**

提供されている変数のいずれかをドロップダウン リストから選択できます。また、変数を作成できます。ドロップダウン リストからは、次の変数を選択します。

表 12-3　クライアントレス SSL VPN の変数

番号	変数置換	定義
1	CSCO_WEBVPN_USERNAME	SSL VPN ユーザ ログイン ID。
2	CSCO_WEBVPN_PASSWORD	SSL VPN ユーザ ログイン パスワード。
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN ユーザ内部リソース パスワード。キャッシュされたクレデンシャルであり、AAA サーバによって認証されていません。ユーザがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN ユーザ ログイン グループ ドロップダウン、接続プロファイル内のグループ エイリアス
5	CSCO_WEBVPN_MACRO1	RADIUS/LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。 RADIUS 経由での変数置換は、VSA#223 によって行われます。

表 12-3　クライアントレス SSL VPN の変数

番号	変数置換	定義
6	CSCO_WEBVPN_MACRO2	RADIUS/LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。 RADIUS 経由での変数置換は、VSA#224 によって行われます。
7	CSCO_WEBVPN_PRIMARY_USERNAME	二重認証用のプライマリ ユーザのログイン ID
8	CSCO_WEBVPN_PRIMARY_PASSWORD	二重認証用のプライマリ ユーザのログイン パスワード
9	CSCO_WEBVPN_SECONDARY_USERNAME	二重認証用のセカンダリ ユーザのログイン ID
10	CSCO_WEBVPN_SECONDARY_PASSWORD	二重認証用のセカンダリ ユーザのログイン ID

ASA が、これら 6 つの変数文字列のいずれかをエンドユーザ要求（ブックマークまたはポストフォーム）で認識すると、リモート サーバに要求を渡す前に、ユーザ固有の値で変数を置換します。

（注） プレーン テキストで（セキュリティ アプライアンスを使用せずに）HTTP Sniffer トレースを実行すると、任意のアプリケーションの http-post パラメータを取得できます。次のリンクから、無料のブラウザ キャプチャ ツールである HTTP アナライザを入手できます。
http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe

変数 1 ～ 4 の使用

ASA は、[SSL VPN Login] ページから最初の 4 つの置き換えの値を取得します。それには、ユーザ名、パスワード、内部パスワード（オプション）、およびグループのフィールドが含まれます。ユーザ要求内のこれらのストリングを認識し、このストリングをユーザ固有の値で置き換えてから、リモート サーバに要求を渡します。

たとえば、URL リストに http://someserver/homepage/CSCO_WEBVPN_USERNAME.html というリンクが含まれていると、ASA はこのリンクを次の一意のリンクに変換します。

- USER1 の場合、リンクは http://someserver/homepage/USER1.html になります。
- USER2 の場合、リンクは http://someserver/homepage/USER2.html になります。

cifs://server/users/CSCO_WEBVPN_USERNAME の場合、ASA は、次のようにファイル ドライブを特定のユーザにマップできます。

- USER1 の場合、リンクは cifs://server/users/USER1 になります。
- USER2 の場合、リンクは cifs://server/users/USER2 になります。

変数 5 および 6 の使用

マクロ 5 および 6 の値は、RADIUS または LDAP のベンダー固有属性（VSA）です。これらにより、RADIUS または LDAP サーバのいずれかで設定した代わりの設定を使用できるようになります。

変数 7 ～ 10 の使用

ASA が、これら 4 つの変数文字列のいずれかをエンドユーザ要求（ブックマークまたはポストフォーム）で認識すると、リモート サーバに要求を渡す前に、ユーザ固有の値で変数を置換します。

ホーム ページの設定例

次の例では、ホーム ページの URL を設定します。

- WebVPN-Macro-Value1 (ID=223), type string, は、*wwwin-portal.example.com* として返されます。
- WebVPN-Macro-Value2 (ID=224), type string, は *401k.com* として返されます。

ホーム ページの値を設定するには、次のように変数置換を設定します。

https://CSCO_WEBVPN_MACRO1。これは、https://wwwin-portal.example.com に変換されます。

この場合の最善の方法は、ASDM で Homepage URL パラメータを設定することです。スクリプトを記述したり何かをアップロードしなくても、管理者はグループ ポリシー内のどのページがスマート トンネル経由で接続するかを指定できます。

ASDM の Network Client SSL VPN または Clientless SSL VPN Access セクションから、[Add/Edit Group Policy] ペインに移動します。パスは次のとおりです。

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit Group Policy] > [Advanced] > [SSL VPN Client] > [Customization] > [Homepage URL] 属性
- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit Group Policy] > [More Options] > [Customization] > [Homepage URL] 属性

ブックマークまたは URL エントリの設定例

SSL VPN 認証で RSA ワンタイム パスワード（OTP）を使用し、続いて OWA 電子メール アクセスでスタティックな内部パスワードを使用することによって、HTTP Post を使用して OWA リソースにログインできます。この場合の最善の方法は、ASDM でブックマーク エントリを追加または編集することです。

次のパスを含め、[Add Bookmark Entry] ペインへのパスは数通り存在します。

- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] > [Add/Edit Bookmark Lists] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters]（URL Method 属性の [Post] をクリックすると表示されます）
- [Network (Client) Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [URL Lists] タブ > [Manage] ボタン > [Configured GUI Customization Objects] > [Add/Edit] ボタン > [Add/Edit Bookmark List] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters]

ファイル共有（CIFS）URL 置換の設定の設定例

CIFS URL の変数置換を使用すると、より柔軟なブックマーク設定を行えます。

URL cifs://server/CSCO_WEBVPN_USERNAME を設定すると、ASA はそれをユーザのファイル共有ホーム ディレクトリに自動的にマッピングします。この方法では、パスワードおよび内部パスワード置換も行えます。次に、URL 置換の例を示します。

cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server

cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server

cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server

cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server

cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server/CSCO_WEBVPN_USERNAME

cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server/CSCO_WEBVPN_USERNAME

外部ポートのカスタマイズ

事前設定されたポータルを使用する代わりに、外部ポータル機能を使用して独自のポータルを作成できます。独自のポータルを設定する場合、クライアントレス ポータルをバイパスし、POST 要求を送信してポータルを取得できます。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Customization] を選択します。必要なカスタマイゼーションを強調表示し、[Edit] を選択します。

ステップ 2　[Enable External Portal] チェックボックスをオンにします。

ステップ 3　[URL] フィールドに、POST 要求が許可されるように、必要な外部ポータルを入力します。

CHAPTER 13

ポリシー グループ

スマート トンネル アクセスの設定

次の項では、クライアントレス SSL VPN セッションでスマート トンネル アクセスをイネーブルにする方法、それらのアクセスを提供するアプリケーションの指定、および使用上の注意について説明します。

スマート トンネル アクセスの設定

スマート トンネル アクセスを設定するには、スマート トンネル リストを作成します。このリストには、スマート トンネル アクセスに適した 1 つ以上のアプリケーション、およびこのリストに関連付けられたエンドポイント オペレーティング システムを含めます。各グループ ポリシーまたはローカル ユーザ ポリシーでは 1 つのスマート トンネル リストがサポートされているため、ブラウザベースではないアプリケーションをサポート対象とするために、グループ化してスマート トンネル リストに加える必要があります。リストを作成したら、1 つ以上のグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。

次の項では、スマート トンネルおよびその設定方法について説明します。

- 「スマート トンネルについて」
- 「スマート トンネルを使用する理由」
- 「スマート トンネルの設定（Lotus の例）」
- 「トンネリングするアプリケーションの設定の簡略化」
- 「スマート トンネル リストについて」
- 「スマート トンネル自動サインオン サーバ リストの作成」
- 「スマート トンネル自動サインオン サーバ リストへのサーバの追加」
- 「スマート トンネル アクセスのイネーブル化とオフへの切り替え」

スマート トンネルについて

スマート トンネルは、TCP ベースのアプリケーションとプライベート サイト間の接続です。このスマート トンネルは、セキュリティ アプライアンスをパスウェイとして、また、ASA をプロキシ サーバとして使用するクライアントレス（ブラウザベース）SSL VPN セッションを使用します。スマート トンネル アクセスを許可するアプリケーションを特定し、各アプリケーションのローカル パスを指定できます。Microsoft Windows で実行するアプリケーションの場合は、チェックサムの SHA-1 ハッシュの一致を、スマート トンネル アクセスを許可する条件として要求もできます。

Lotus SameTime および Microsoft Outlook は、スマート トンネル アクセスを許可するアプリケーションの例です。

スマート トンネルを設定するには、アプリケーションがクライアントであるか、Web 対応アプリケーションであるかに応じて、次の手順のいずれかを実行する必要があります。

- クライアント アプリケーションの 1 つ以上のスマート トンネル リストを作成し、スマート トンネル アクセスを必要とするグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。
- スマート トンネル アクセスに適格な Web 対応アプリケーションの URL を指定する 1 つ以上のブックマーク リスト エントリを作成し、スマート トンネル アクセスを必要とするグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。

また、クライアントレス SSL VPN セッションを介したスマート トンネル接続でのログイン クレデンシャルの送信を自動化する Web 対応アプリケーションのリストも作成できます。

スマート トンネルを使用する理由

スマート トンネル アクセスでは、クライアントの TCP ベースのアプリケーションは、ブラウザベースの VPN 接続を使用してサービスにアクセスできます。この方法では、プラグインやレガシー テクノロジーであるポート転送と比較して、ユーザには次のような利点があります。

- スマート トンネルは、プラグインよりもパフォーマンスが向上します。
- ポート転送とは異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続を要求しないことにより、ユーザ エクスペリエンスが簡略化されます。
- ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。

プラグインの利点は、クライアント アプリケーションをリモート コンピュータにインストールする必要がないという点です。

前提条件

ASA Release 9.0 のスマート トンネルでサポートされているプラットフォームおよびブラウザについては、『*Supported VPN Platforms, Cisco ASA Series*』を参照してください。

次の要件と制限事項が Windows でのスマート トンネル アクセスには適用されます。

- Windows では ActiveX または Oracle Java ランタイム環境（JRE）4 Update 15 以降（JRE 6 以降を推奨）をブラウザでイネーブルにしておく必要がある。
- Winsock 2 の TCP ベースのアプリケーションだけ、スマート トンネル アクセスに適する。
- Mac OS X の場合に限り、Java Web Start をブラウザでイネーブルにしておく必要がある。

制約事項

- スマート トンネルは、Microsoft Windows を実行しているコンピュータとセキュリティ アプライアンス間に配置されたプロキシだけをサポートする。スマート トンネルは、Windows でシステム全体のパラメータを設定する Internet Explorer 設定を使用します。この設定がプロキシ情報を含む場合があります。
  - Windows コンピュータで、プロキシが ASA にアクセスする必要がある場合は、クライアントのブラウザにスタティック プロキシ エントリが必要であり、接続先のホストがクライアントのプロキシ例外のリストに含まれている必要があります。
  - Windows コンピュータで、プロキシが ASA にアクセスする必要がなく、プロキシがホスト アプリケーションにアクセスする必要がある場合は、ASA がクライアントのプロキシ例外のリストに含まれている必要があります。

  プロキシ システムはスタティック プロキシ エントリまたは自動設定のクライアントの設定、または PAC ファイルによって定義できます。現在、スマート トンネルでは、スタティック プロキシ設定だけがサポートされています。
- スマート トンネルでは、Kerberos Constrained Delegation（KCD）はサポートされない。
- Windows の場合、コマンド プロンプトから開始したアプリケーションにスマート トンネル アクセスを追加する場合は、スマート トンネル リストの 1 つのエントリの [Process Name] に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要があります。これは「cmd.exe」がアプリケーションの親であるためです。
- HTTP ベースのリモート アクセスによって、いくつかのサブネットが VPN ゲートウェイへのユーザ アクセスをブロックすることがある。これを修正するには、Web とエンドユーザの場所との間のトラフィックをルーティングするために ASA の前にプロキシを配置します。このプロキシが CONNECT 方式をサポートしている必要があります。認証が必要なプロキシの場合、スマート トンネルは、基本ダイジェスト認証タイプだけをサポートします。
- スマート トンネルが開始されると、ASA は、ブラウザ プロセスが同じである場合に VPN セッション経由ですべてのブラウザ トラフィックをデフォルトで送信する。また、tunnel-all ポリシーが適用されている場合にのみ、ASA は同じ処理を行います。ユーザがブラウザ プロセスの別のインスタンスを開始すると、VPN セッション経由ですべてのトラフィックが送信されます。ブラウザ プロセスが同じで、セキュリティ アプライアンスが URL へのアクセスを提供しない場合、ユーザはその URL を開くことはできません。回避策として、tunnel-all ではないトンネル ポリシーを割り当てます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されない。ユーザはフェールオーバー後に再接続する必要があります。
- スマート トンネルの Mac バージョンは、POST ブックマーク、フォームベースの自動サインオン、または POST マクロ置換をサポートしない。
- Mac OS ユーザの場合、ポータル ページから起動されたアプリケーションだけがスマート トンネル セッションを確立できる。この要件には、Firefox に対するスマート トンネルのサポートも含まれます。スマート トンネルを最初に使用する際に、Firefox を使用して Firefox の別のインスタンスを起動するには、csco_st という名前のユーザ プロファイルが必要です。このユーザ プロファイルが存在しない場合、セッションでは、作成するようにユーザに要求します。
- Mac OS X では、SSL ライブラリにダイナミックにリンクされた、TCP を使用するアプリケーションをスマート トンネルで使用できる。

- Mac OS X では、スマート トンネルは次をサポートしない。
  - プロキシ サービス
  - 自動サインオン
  - 2 つのレベルの名前スペースを使用するアプリケーション
  - Telnet、SSH、cURL などのコンソールベースのアプリケーション
  - dlopen または dlsym を使用して libsocket コールを見つけ出すアプリケーション
  - libsocket コールを見つけ出すスタティックにリンクされたアプリケーション
- Mac OS X では、プロセスへのフル パスが必要である。また、このパスは大文字と小文字が区別されます。各ユーザ名のパスを指定しないようにするには、部分パスの前にチルダ（~）を入力します（例：~/bin/vnc）。

スマート トンネルの設定（Lotus の例）

（注） この例では、アプリケーションでのスマート トンネル サポートを追加するために必要な最小限の指示だけを示します。詳細については、以降の各項にあるフィールドの説明を参照してください。

手順の詳細

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] を選択します。

ステップ 2　アプリケーションを追加するスマート トンネル リストをダブルクリックするか、または [Add] をクリックしてアプリケーションのリストを作成し、[List Name] フィールドにそのリストの名前を入力して [Add] をクリックします。

たとえば、[Smart Tunnels] ペインで [Add] をクリックし、[List Name] フィールドに **Lotus** と入力して [Add] をクリックします。

ステップ 3　[Add or Edit Smart Tunnel List] ダイアログボックスで [Add] をクリックします。

ステップ 4　[Application ID] フィールドに、スマート トンネル リスト内のエントリに対する一意のインデックスとして使用する文字列を入力しします。

ステップ 5　[Process Name] ダイアログボックスに、ファイル名とアプリケーションの拡張子を入力します。

表 13-1 に、[Application ID] 文字列の例と、Lotus をサポートするために必要となる関連付けられたパスを示します。

表 13-1　スマート トンネルの例 : Lotus 6.0 Thick Client with Domino Server 6.5.5

アプリケーション ID の例	必要最小限のプロセス名
lotusnotes	notes.exe
lotusnlnotes	nlnotes.exe
lotusntaskldr	ntaskldr.exe
lotusnfileret	nfileret.exe

ステップ 6　[OS] の横の [Windows] を選択します。

ステップ 7　[OK] をクリックします。

ステップ 8　リストに追加するアプリケーションごとに、ステップ 3 ～ 7 を繰り返します。

ステップ 9　[Add or Edit Smart Tunnel List] ダイアログボックスで [OK] をクリックします。

ステップ 10　次のようにして、関連付けられたアプリケーションへのスマート トンネル アクセスを許可するグループ ポリシーとローカル ユーザ ポリシーにリストを割り当てます。

- グループ ポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add] または [Edit] > [Portal] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。
- ローカル ユーザ ポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] または [Edit] > [VPN Policy] > [Clientless SSL VPN] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。

トンネリングするアプリケーションの設定の簡略化

スマート トンネル アプリケーション リストは、基本的に、トンネルへのアクセスを許可するアプリケーションのフィルタです。デフォルトでは、ブラウザによって開始されるすべてのプロセスに対してアクセスが許可されます。スマート トンネル対応ブックマークによって、クライアントレス セッションでは Web ブラウザによって開始されるプロセスのみにアクセスが許可されます。ブラウザ以外のアプリケーションでは、管理者はすべてのアプリケーションをトンネリングすることを選択して、エンド ユーザがどのアプリケーションを起動するかを知る必要性をなくすことができます。表 13-2 にアクセスを許可されるプロセスの状況を示します。

表 13-2　スマート トンネル アプリケーションのアクセスと対応ブックマーク

状況	スマート トンネル対応ブックマーク	スマート トンネル アプリケーション アクセス
アプリケーション リストが指定される	アプリケーション リストのプロセス名と一致する任意のプロセスにアクセス権が付与されます。	アプリケーション リストのプロセス名と一致するプロセスのみにアクセス権が付与されます。
スマート トンネルをオフに切り替える	すべてのプロセス（およびその子プロセス）にアクセス権が付与されます。	プロセスにアクセス権は付与されません。
[Smart Tunnel all Applications] チェックボックスをオンにします。	すべてのプロセス（およびその子プロセス）にアクセス権が付与されます。 **（注）** スマート トンネル以外の Web ページによって開始されたプロセスも含まれます（Web ページが同じブラウザ プロセスによって処理される場合）。	ブラウザを開始したユーザが所有するすべてのプロセスにアクセス権が付与されますが、その子プロセスには付与されません。

制約事項

この設定は、Windows プラットフォームのみに適用されます。

手順の詳細

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

ステップ 2　[User Account] ウィンドウで、編集するユーザ名を強調表示します。

ステップ 3　[Edit] をクリックします。[Edit User Account] ウィンドウが表示されます。

ステップ 4　[Edit User Account] ウィンドウの左側のサイドバーで、[VPN Policy] > [Clientless SSL VPN] をクリックします。

ステップ 5　次のいずれかの操作を行います。

- [smart tunnel_all_applications] チェックボックスをオンにします。リストを作成しなくても、または外部アプリケーションについてエンド ユーザが起動する可能性がある実行ファイルを知らなくても、すべてのアプリケーションがトンネリングされます。
- または、次のトンネル ポリシー オプションから選択します。
  - [Smart Tunnel Policy] パラメータの [Inherit] チェックボックスをオフにします。
  - ネットワーク リストから選択し、トンネル オプションの 1 つを指定します。指定されたネットワークに対してスマート トンネルを使用する、指定されたネットワークに対してスマート トンネルを使用しない、またはすべてのネットワーク トラフィックに対してトンネルを使用する、のいずれかです。

スマート トンネル アクセスに適格なアプリケーションの追加

各 ASA のクライアントレス SSL VPN コンフィギュレーションは、*スマート トンネル リスト*をサポートしています。各リストは、スマート トンネル アクセスに適格な 1 つ以上のアプリケーションを示します。各グループ ポリシーまたはユーザ名は 1 つのスマート トンネル リストのみをサポートするため、サポートされる各アプリケーションのセットをスマート トンネル リストにグループ化する必要があります。

[Add or Edit Smart Tunnel Entry] ダイアログボックスでは、スマート トンネル リストにあるアプリケーションの属性を指定できます。

ステップ 1　[Configuration] > [Remote Access VPN] >[Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に進み、編集するスマート トンネル アプリケーション リストを選択するか、新しいリストを追加します。

ステップ 2　新しいリストの場合は、アプリケーションまたはプログラムのリストに付ける一意の名前を入力します。スペースは使用しないでください。

スマート トンネル リストのコンフィギュレーションに続いて、クライアントレス SSL VPN のグループ ポリシーとローカル ユーザ ポリシーの [Smart Tunnel List] 属性の横にリスト名が表示されます。他に設定する可能性があるリストと、内容および目的を区別できるような名前を付けてください。

ステップ 3　[Add] をクリックして、このスマート トンネル リストに必要な数のアプリケーションを追加します。パラメータについては次で説明します。

- [Application ID]：スマート トンネル リストのエントリに命名する文字列を入力します。このユーザ指定の名前は保存され、GUI に戻されます。文字列はオペレーティング システムに対して一意です。通常は、スマート トンネル アクセスを許可されるアプリケーションに付けられる名前です。異なるパスまたはハッシュ値を指定するアプリケーションの複数バージョンをサポートするには、この属性を使用してエントリを差別化し、オペレーティング システム、および各リスト エントリによってサポートされているアプリケーションの名前とバージョンの両方を指定します。文字列は最大 64 文字まで使用できます。
- [Process Name]：アプリケーションのファイル名またはパスを入力します。ストリングには最大 128 文字を使用できます。

  Windows では、アプリケーションにスマート トンネル アクセスを許可する場合に、この値とリモート ホストのアプリケーション パスの右側の値が完全に一致している必要があります。Windows でファイル名のみを指定すると、SSL VPN では、アプリケーションにスマート トンネル アクセスを許可する場合に、リモート ホストに対して場所の制限を強制しません。

  アプリケーションのパスを指定し、ユーザが別の場所にインストールした場合は、そのアプリケーションは許可されません。アプリケーションは、入力する値と文字列と右側の値が一致している限り、任意のパスに配置できます。

  アプリケーションがリモート ホストの複数のパスのいずれかにある場合に、アプリケーションにスマート トンネル アクセスを認可するには、このフィールドにアプリケーションの名前と拡張子だけを指定するか、またはパスごとに固有のスマート トンネル エントリを作成します。

（注） スマート トンネル アクセスで突然問題が発生する場合、[Process Name] 値がアップグレードされたアプリケーションに対して最新ではない可能性があります。たとえば、アプリケーションへのデフォルト パスは、そのアプリケーションおよび次のアップグレード版を製造する企業が買収されると変更されることがあります。

  Windows の場合、コマンド プロンプトから開始したアプリケーションにスマート トンネル アクセスを追加する場合は、スマート トンネル リストの 1 つのエントリの [Process Name] に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要があります。これは「cmd.exe」がアプリケーションの親であるためです。

- [OS]：[Windows] または [Mac] をクリックし、アプリケーションのホスト オペレーティング システムを指定します。
- [Hash]（任意、Windows にのみ該当）：この値を取得するには、アプリケーションのチェックサム（つまり、実行ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュを計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft ファイル チェックサム整合性検証（FCIV）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。FCIV のインストール後、スペースを含まないパス（c:/fciv.exe など）に、ハッシュするアプリケーションの一時コピーを置き、コマンドラインで **fciv.exe -sha1** *application* と入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。

  SHA-1 ハッシュは、常に 16 進数 40 文字です。

  クライアントレス SSL VPN は、アプリケーションにスマート トンネル アクセスの認可を与える前に、[Application ID] に一致するアプリケーションのハッシュを計算します。結果が [Hash] の値と一致すれば、アプリケーションにスマート トンネル アクセスの資格を与えます。

ハッシュを入力することにより、[Application ID] で指定した文字列に一致する不正ファイルに対して SSL VPN が資格を与えないようしています。チェックサムは、アプリケーションのバージョンまたはパッチによって異なるため、入力する [Hash] 値は、リモート ホストの 1 つのバージョンやパッチにしか一致しない可能性があります。複数のバージョンのアプリケーションにハッシュを指定するには、[Hash] 値ごとに固有のスマート トンネル エントリを作成します。

（注） [Hash] 値を入力し、スマート トンネル アクセスで、アプリケーションの今後のバージョンまたはパッチをサポートする必要がある場合は、スマート トンネル リストを更新し続ける必要があります。スマート トンネル アクセスに突然問題が発生した場合は、[Hash] 値を含むアプリケーション リストが、アプリケーションのアップグレードによって最新の状態になっていない可能性があります。この問題は hash を入力しないことによって回避できます。

ステップ 4　[OK] をクリックしてアプリケーションを保存し、このスマート トンネル リストに必要な数だけアプリケーションを作成します。

ステップ 5　スマート トンネル リストの作成が終わったら、そのリストをアクティブにするには、次の手順に従って、グループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てる必要があります。

- グループ ポリシーにリストを割り当てるには、[Config] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add] または [Edit] > [Portal] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。
- ローカル ユーザ ポリシーにリストを割り当てるには、[Config] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] または [Edit] > [VPN Policy] > [Clientless SSL VPN] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。

表 13-3　スマート トンネル エントリの例

スマート トンネルのサポート	アプリケーション ID（一意の文字列であればどれでも OK）	プロセス名	OS
Mozilla Firefox	firefox	firefox.exe	Windows
Microsoft Outlook Express	outlook-express	msimn.exe	Windows
より制限的なオプション：実行ファイルが事前定義済みのパスにある場合は、Microsoft Outlook Express 専用。	outlook-express	\Program Files\Outlook Express\msimn.exe	Windows
Mac で新しいターミナル ウィンドウを開く（ワンタイムパスワードが実装されているので、それ以降、同じターミナル ウィンドウでのアプリケーションの起動は失敗します）。	terminal	Terminal	Mac
新しいウィンドウでスマート トンネルを開始	new-terminal	Terminal open -a MacTelnet	Mac
Mac ターミナル ウィンドウでアプリケーションを起動	curl	Terminal curl www.example.com	Mac

スマート トンネル リストについて

グループ ポリシーとユーザ名ごとに、次のいずれかを行うようにクライアントレス SSL VPN を設定できます。

- ユーザのログイン時に自動的にスマート トンネル アクセスを開始する。
- ユーザのログイン時にスマート トンネル アクセスをイネーブルにするが、ユーザはクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、スマート トンネル アクセスを手動で開始するようにユーザに要求する。

制約事項

スマート トンネル ログオン オプションは、各グループ ポリシーとユーザ名に対して互いに排他的です。1 つだけ使用してください。

スマート トンネル自動サインオン サーバ リストの作成

[Add Smart Tunnel Auto Sign-on Server List] ダイアログボックスで、スマート トンネルのセットアップ中にログイン クレデンシャルの送信を自動化するサーバのリストを追加または編集できます。スマート トンネルの自動サインオンは、Internet Explorer および Firefox で利用可能です。

ステップ 1　[Configuration] > [Remote Access VPN] >[Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に進み、[Smart Tunnel Auto Sign-on Server List] が展開されて表示されていることを確認します。

ステップ 2　[Add] をクリックして、他に設定する可能性があるリストと、内容および目的を区別できるようなリモート サーバのリストの一意の名前を入力します。文字列は最大 64 文字まで使用できます。スペースは使用しないでください。

スマート トンネルの自動サインオン リストを作成した後は、クライアントレス SSL VPN グループ ポリシーおよびローカル ポリシー コンフィギュレーションの下の [Auto Sign-on Server List] 属性の横に、リスト名が表示されます。

スマート トンネル自動サインオン サーバ リストへのサーバの追加

次の手順では、スマート トンネル接続での自動サインオンを提供するサーバのリストにサーバを追加し、そのリストをグループ ポリシーまたはローカル ユーザに割り当てる方法について説明します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に進み、リストのいずれかを選択して、[Edit] をクリックします。

ステップ 2　[Tunnel Auto Sign-On Server List] ダイアログで [Add] ボタンをクリックして、スマート トンネル サーバをもう 1 つ追加します。

ステップ 3　自動認証を行うサーバのホスト名または IP アドレスを入力します。

- [Hostname] を選択する場合、自動認証を行うホスト名またはワイルドカード マスクを入力します。次のワイルドカード文字を使用できます。
  - *：任意の数の文字を一致させる、またはどの文字も一致させない。
  - ?：単一の文字を一致させる。

- [ ] : かっこ内に指定された範囲内の、任意の 1 文字を一致させる。
- たとえば、*.example.com と入力します。このオプションを使用すると、IP アドレスのダイナミックな変更からコンフィギュレーションを保護します。

- [IP Address] を選択する場合、IP アドレスを入力します。

（注）　Firefox では、ワイルドカードを使用したホスト マスク、IP アドレスを使用したサブネット、またはネットマスクをサポートしていません。正確なホスト名または IP アドレスを使用する必要があります。たとえば、Firefox では、*.cisco.com を入力した場合、email.cisco.com をホストする自動サインオンは失敗します。

ステップ 4　[Windows Domain]（オプション）：認証で必要な場合、クリックして Windows ドメインをユーザ名に追加します。このオプションを使用する場合は、1 つ以上のグループ ポリシーまたはローカル ユーザ ポリシーにスマート トンネル リストを割り当てる際に、ドメイン名を指定する必要があります。

ステップ 5　[HTTP-based Auto Sign-On]（オプション）

- [Authentication Realm] : レルムは Web サイトの保護領域に関連付けられ、認証時に認証プロンプトまたは HTTP ヘッダーのいずれかでブラウザに再度渡されます。ここで自動サインオンが設定され、レルムの文字列が指定されたら、ユーザはレルムの文字列を Web アプリケーション（Outlook Web Access など）で設定し、Web アプリケーションにサインオンすることなくアクセスできます。

  イントラネットの Web ページのソース コードで使用されるアドレス形式を使用します。ブラウザ アクセス用にスマート トンネル自動サインオンを設定しており、一部の Web ページでホスト名が使用され、他の Web ページで IP アドレスが使用されている場合、あるいはどちらが使用されているかわからない場合は、両方を異なるスマート トンネル自動サインオン エントリで指定します。それ以外の場合、Web ページのリンクで、指定されたフォーマットとは異なるフォーマットが使用されると、ユーザがリンクをクリックしても開きません。

（注）　対応するレルムがわからない場合、管理者はログインを一度実行し、プロンプト ダイアログから文字列を取得する必要があります。

- [Port Number] : 対応するホストのポート番号を指定します。Firefox では、ポート番号が指定されていない場合、自動サインオンはデフォルトのポート番号 80 および 443 でそれぞれアクセスされた HTTP および HTTPS に対して実行されます。

ステップ 6　[OK] をクリックします。

ステップ 7　スマート トンネル自動サインオン サーバ リストのコンフィギュレーションに続いて、そのリストをアクティブにするには、グループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てる必要があります。

- グループ ポリシーにリストを割り当てるには、次の手順を実行します。
  1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] の順に進み、グループ ポリシーを開きます。
  2. [Portal] タブを選択し、[Smart Tunnel] 領域を見つけ、[Auto Sign-on Server List] 属性の横にあるドロップダウン リストから自動サインオン サーバ リストを選択します。

- ローカル ユーザ ポリシーにリストを割り当てるには、次の手順を実行します。
  1. [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択し、自動サインオン サーバ リストに割り当てるローカル ユーザを編集します。
  2. [VPN Policy] > [Clientless SSL VPN] 順に進み、[Smart Tunnel] 領域の下の [Auto Sign-on Server] 設定を探します。
  3. [Inherit] をオフにし、[Auto Sign-on Server List] 属性の横にあるドロップダウン リストからサーバ リストを選択します。

スマート トンネル アクセスのイネーブル化とオフへの切り替え

デフォルトでは、スマート トンネルはオフになっています。

スマート トンネル アクセスをイネーブルにしている場合、ユーザは、クライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、スマート トンネル アクセスを手動で開始する必要があります。

スマート トンネルからのログオフの設定

ここでは、スマート トンネルからの適切なログオフ方法について説明します。すべてのブラウザ ウィンドウを閉じるか、通知アイコンを右クリックしてログアウトを確認すると、スマート トンネルからログオフできます。

（注） ポータルにあるログアウト ボタンを使用することを強くお勧めします。この方法は、クライアントレス SSL VPN 用であり、スマート トンネルが使用されているかどうかに関係なくログオフが行われます。通知アイコンは、ブラウザを使用しないスタンドアロン アプリケーションを使用する場合に限り使用する必要があります。

ペアレント プロセスの終了

この方法では、ログオフを示すためにすべてのブラウザを閉じることが必要です。スマート トンネルのライフタイムは現在、プロセスのライフタイムの開始に結び付けられています。たとえば、Internet Explorer からスマート トンネルと開始した場合、iexplore.exe が実行されていないとスマート トンネルがオフになります。スマート トンネルは、ユーザがログアウトせずにすべてのブラウザを閉じた場合でも、VPN セッションが終了したと判断します。

（注） 場合によっては、ブラウザ プロセスがエラーの結果として、意図的にではなく残っていることがあります。また、Secure Desktop を使用しているときに、ユーザが Secure Desktop 内ですべてのブラウザを閉じてもブラウザ プロセスが別のデスクトップで実行されている場合があります。したがって、スマート トンネルは、現在のデスクトップで表示されているウィンドウがない場合にすべてのブラウザ インスタンスが終了したと見なします。

通知アイコンの利用

ブラウザを閉じてもセッションが失われないようにするために、ペアレント プロセスの終了時にログオフをオフに切り替えることもできます。この方法では、システム トレイの通知アイコンを使用してログアウトします。アイコンは、ユーザがアイコンをクリックしてログアウトするまで維持されます。ユーザがログアウトする前にセッションの期限が切れた場合、アイコンは、次回に接続を試行するまで維持されます。セッション ステータスがシステム トレイで更新されるまで時間がかかることがあります。

（注） このアイコンが、SSL VPN からログアウトする別の方法です。これは、VPN セッション ステータスのインジケータではありません。

手順の詳細

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] を選択します。

ステップ 2　[Click on smart-tunnel logoff icon in the system tray] オプション ボタンをイネーブルにします。

ステップ 3　ウィンドウの [Smart Tunnel Networks] 部分で、[Add] をオンにして、アイコンを含めるネットワークの IP アドレスとホスト名の両方を入力します。

（注） アイコンを右クリックすると、SSL VPN からのログアウトをユーザに求める単一のメニュー項目が表示されます。

プロキシ バイパスの使用

ユーザはプロキシ バイパスを使用するように ASA を設定できます。これは、プロキシ バイパスが提供する特別なコンテンツ リライト機能を使用した方が、アプリケーションや Web リソースをより有効活用できる場合に設定します。プロキシ バイパスはコンテンツのリライトに代わる手法であり、元のコンテンツの変更を最小限に抑えます。多くの場合、カスタム Web アプリケーションでこれを使用すると有効です。

プロキシ バイパスには複数のエントリを設定できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートにより、プロキシ バイパス ルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシ バイパスを設定する場合、ネットワーク コンフィギュレーションによっては、これらのポートが ASA にアクセスできるようにするために、ファイアウォール コンフィギュレーションの変更が必要になることがあります。この制限を回避するには、パス マスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスは、URL で .com や .org、またはその他のタイプのドメイン名の後に続く全体です。たとえば、www.example.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.example.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、*（ワイルドカード）を /hr* のように使用して、コマンドを複数回使用しないようにできます。

ASA がコンテンツ リライトをほとんどまたはまったく実行しない場合のルールを設定できます。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Proxy Bypass] の順に進みます。

ステップ 2　プロキシ バイパスのインターフェイス名を選択します。

ステップ 3　プロキシ バイパス用のポートまたは URI を指定します。

- [Port]：（オプション ボタン）プロキシ バイパスにポートを使用します。有効なポート番号は 20000 ～ 21000 です。
- [Port]：（フィールド）ASA がプロキシ バイパス用に予約する大きな番号のポートを入力します。
- [Path Mask]：（オプション ボタン）プロキシ バイパスに URL を使用します。
- [Path Mask]：（フィールド）プロキシ バイパス用の URL を入力します。この URL には、正規表現を使用できます。

ステップ 4　プロキシ バイパスのターゲット URL を定義します。

- [URL]：（ドロップダウン リスト）プロトコルとして、http または https をクリックします。
- [URL]（テキスト フィールド）：プロキシ バイパスを適用する URL を入力します。

ステップ 5　リライトするコンテンツを指定します。選択肢は、なし、または XML、リンク、およびクッキーの組み合わせです。

- [XML]：XML コンテンツをリライトする場合に選択します。
- [Hostname]：リンクをリライトする場合に選択します。

ポータル アクセス ルールの設定

この拡張機能により、カスタマーは、HTTP ヘッダー内に存在するデータに基づいて、クライアントレス SSL VPN セッションを許可または拒否するグローバルなクライアントレス SSL VPN アクセス ポリシーを設定することができます。ASA がクライアントレス SSL VPN セッションを拒否する場合、ただちにエンドポイントにエラー コードを返します。

ASA は、このアクセス ポリシーを、エンドポイントが ASA に対して認証する前に評価します。その結果、拒否の場合は、エンドポイントからの追加の接続試行による ASA の処理リソースの消費はより少なくなります。

前提条件

ASA にログインし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は次のプロンプトを表示します。

```
hostname(config)#
```

手順の詳細

ステップ 1　ASDM を起動し、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Portal Access Rule] を選択します。

[Portal Access Rule] ウィンドウが開きます。

ステップ 2　[Add] をクリックしてポータル アクセス ルールを作成するか、既存のルールを選択して [Edit] をクリックします。

[Add Portal Access Rule] または [Edit Portal Access Rule] ダイアログボックスが開きます。

ステップ 3　1 ～ 65535 のルール番号を [Rule Priority] フィールドに入力します。

ルールは 1 ～ 65535 のプライオリティの順序で処理されます。

ステップ 4　[User Agent] フィールドに、HTTP ヘッダーで検索するユーザ エージェントの名前を入力します。

- 文字列を広範囲に指定するには、文字列をワイルドカード（*）で囲みます。たとえば、*Thunderbird* です。検索文字列でワイルドカードを使用することを推奨します。ワイルドカードを使用しないと、ルールがどの文字列とも一致しないか、予期したよりも大幅に少ない文字列としか一致しない場合があります。
- 文字列にスペースが含まれている場合、ASDM によって、ルールの保存時に文字列の最初と最後に自動的に引用符が追加されます。たとえば、`my agent` と入力した場合、ASDM によってこの文字列は `"my agent"` として保存されます。ASA では `my agent` の一致が検索されます。

  スペースを含む文字列に引用符を追加しないでください。ただし、文字列に追加した引用符を ASA で照合させる場合を除きます。たとえば、`"my agent"` と入力すると、ASDM はその文字列を `"\"my agent\'"` として保存するため、`"my agent"` を検出しようとしますが、`my agent` は見つかりません。
- スペースを含む文字列でワイルドカードを使用する場合は、文字列全体をワイルドカードで開始して終了します。たとえば、`*my agent*` です。ASDM によって、ルールの保存時に、その文字列は自動的に引用符で囲まれます。

ステップ 5　[Action] フィールドで、[Deny] または [Permit] を選択します。

ASA は、この設定に基づいて、クライアントレス SSL VPN 接続を拒否または許可します。

ステップ 6　HTTP メッセージ コードを [Returned HTTP Code] フィールドに入力します。

HTTP メッセージ番号 403 がフィールドにあらかじめ入力されており、これがポータル アクセス ルールのデフォルト値です。メッセージ コードの有効な範囲は 200 ～ 599 です。

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。

クライアントレス SSL VPN リモート ユーザ

この章では、ユーザ リモート システムの設定要件と作業の概要を説明します。また、ユーザがクライアントレス SSL VPN の使用を開始できるようにします。内容は次のとおりです。

- 「ユーザ名およびパスワード」
- 「セキュリティのヒントの通知」
- 「クライアントレス SSL VPN の機能を使用するためのリモート システムの設定」
- 「クライアントレス SSL VPN データのキャプチャ」

（注） ASA がクライアントレス SSL VPN 用に設定されていることを確認します。

ユーザ名およびパスワード

ネットワークによっては、リモート セッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、クライアントレス SSL VPN、メール サーバ、ファイル サーバ、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。必要なアクセス権があることを確認してください。

表 14-1 に、クライアントレス SSL VPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 14-1　クライアントレス SSL VPN ユーザに通知するユーザ名とパスワード

ログイン ユーザ名/パスワード タイプ	目的	入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN セッションを開始するとき
ファイル サーバ	リモート ファイル サーバへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき

表 14-1　クライアントレス SSL VPN ユーザに通知するユーザ名とパスワード （続き）

ログイン ユーザ名/ パスワード タイプ	目的	入力するタイミング
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	クライアントレス SSL VPN 経由によるリモート メール サーバへのアクセス	電子メール メッセージの送受信

セキュリティのヒントの通知

次のセキュリティのヒントを通知してください。

- クライアントレス SSL VPN セッションから必ずログアウトします。ログアウトするには、クライアントレス SSL VPN ツールバーの logout アイコンをクリックするか、またはブラウザを閉じます。
- クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。クライアントレス SSL VPN は、企業ネットワーク上のリモート コンピュータやワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信はセキュアではありません。

クライアントレス SSL VPN の機能を使用するためのリモート システムの設定

表 14-2 に、クライアントレス SSL VPN を使用するためのリモート システムの設定に関連するタスク、タスクの要件と前提条件、および推奨される使用法を示します。

各ユーザ アカウントを異なる設定にしたことにより、クライアントレス SSL VPN ユーザがそれぞれに使用できる機能が異なる可能性があります。表 14-2 では、情報をユーザ アクティビティ別にまとめています。

表 14-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
クライアントレス SSL VPN の起動	インターネットへの接続	サポートされているインターネット接続は、次のとおりです。 • 家庭の DSL、ケーブル、ダイヤルアップ • 公共のキオスク • ホテルの回線 • 空港の無線ノード • インターネット カフェ
	クライアントレス SSL VPN がサポートされているブラウザ	クライアントレス SSL VPN には、次のブラウザを推奨します。他のブラウザでは、クライアントレス SSL VPN 機能が完全にサポートされていない可能性があります。 Microsoft Windows の場合： • Internet Explorer 8 • Firefox 8 Linux の場合： • Firefox 8 Mac OS X の場合： • Safari 5 • Firefox 8
	ブラウザでイネーブルにされているクッキー	ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
	クライアントレス SSL VPN の URL	HTTPS アドレスの形式は次のとおりです。 https://*address* *address* は、クライアントレス SSL VPN がイネーブルになっている ASA（またはロード バランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、https://10.89.192.163 または https://cisco.example.com のようになります。
	クライアントレス SSL VPN のユーザ名とパスワード	
	（オプション）ローカル プリンタ	クライアントレス SSL VPN は、Web ブラウザからネットワーク プリンタへの印刷をサポートしていません。ローカル プリンタへの印刷はサポートされています。

表 14-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件 （続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
クライアントレス SSL VPN 接続でのフローティング ツールバーの使用		フローティング ツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。 ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。 フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。[Close] ボタンをクリックすると、ASA によってクライアントレス SSL VPN セッションを閉じることを求めるメッセージが表示されます。 **ヒント** テキストをテキスト フィールドに貼り付けるには、Ctrl を押した状態で V を押します （クライアントレス SSL VPN ツールバーでは、右クリックはイネーブルになっていません）。
Web ブラウジング	保護されている Web サイトのユーザ名とパスワード	クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。「セキュリティのヒントの通知」を参照してください。 クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。 • クライアントレス SSL VPN のタイトルバーが各 Web ページの上部に表示される。 • Web サイトへのアクセス方法： – [Clientless SSL VPN Home] ページ上の [Enter Web Address] フィールドに URL を入力する。 – [Clientless SSL VPN Home] ページ上にある設定済みの Web サイト リンクをクリックする。 – 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする。 また、特定のアカウントの設定によっては、次のようになる場合もあります。 • 一部の Web サイトがブロックされている。 • アクセス可能な Web サイトが、[Clientless SSL VPN Home] ページにリンクとして表示されるサイトに限定される。

表 14-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件 （続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
ネットワーク ブラウジングとファイル管理	共有リモート アクセス用に設定されたファイル アクセス権	クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。
	保護されているファイル サーバのサーバ名とパスワード	—
	フォルダとファイルが存在するドメイン、ワークグループ、およびサーバ名	ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。
	—	コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。
アプリケーションの使用 （ポート転送またはアプリケーション アクセスと呼ばれる）	**（注）** Mac OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。	
	（注） この機能を使用するには、Oracle Java Runtime Environment（JRE）をインストールしてローカル クライアントを設定する必要があります。これには、ローカル システムで管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。	
	⚠ **注意** ユーザは、アプリケーションを使用し終えたら、[Close] アイコンをクリックして必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体にアクセスできなくなる可能性があります。	
	インストール済みのクライアント アプリケーション	—
	ブラウザでイネーブルにされているクッキー	—
	管理者特権	ユーザは、DNS 名を使用してサーバを指定する場合、ホスト ファイルを変更するのに必要になるため、コンピュータに対する管理者アクセス権が必要になります。
	インストール済みの Oracle Java Runtime Environment（JRE）バージョン 1.4.x と 1.5.x ブラウザで JavaScript をイネーブルにする必要があります。デフォルトでは有効に設定されています。	JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。 まれに、Java 例外エラーで、ポート転送アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。 1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。 2. Java アイコンがコンピュータのタスク バーに表示されていないことを確認します。Java のインスタンスをすべて閉じます。 3. クライアントレス SSL VPN セッションを確立し、ポート転送 Java アプレットを起動します。

表 14-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
	設定済みのクライアント アプリケーション（必要な場合）。 **（注）** Microsoft Outlook クライアントの場合、この設定手順は不要です。 Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。 Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] の値をチェックします。 • [Remote Server] にサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。 • [Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。	クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。 1. リモート システムでクライアントレス SSL VPN を起動し、[Clientless SSL VPN Home] ページで Application Access リンクをクリックします。[Application Access] ウィンドウが表示されます。 2. [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。 3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。
	（注） クライアントレス SSL VPN で実行されているアプリケーションで URL（電子メール内の URL など）をクリックしても、クライアントレス SSL VPN ではそのサイトは開きません。クライアントレス SSL VPN でこのようなサイトを開くには、[Enter (URL) Address] フィールドに URL をカット アンド ペーストします。	
Application Access を介した電子メールの使用	Application Access の要件を満たす（「アプリケーションの使用」を参照）	電子メールを使用するには、[Clientless SSL VPN Home] ページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。
	（注） IMAP クライアントの使用中にメール サーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。	
	他の電子メール クライアント	Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。 クライアントレス SSL VPN は、Lotus Notes や Eudora などの、ポート転送を介したその他の SMTPS、POP3S、または IMAP4S 電子メール プログラムをサポートしますが、動作確認は行っていません。
電子メール プロキシを介した電子メールの使用	インストールされている Web ベースの電子メール製品	サポートされている製品は次のとおりです。 • Outlook Web Access 最適な結果を得るために、Internet Explorer 8.x 以上、または Firefox 8 で OWA を使用してください。 • Lotus Notes その他の Web ベースの電子メール製品も動作しますが、動作確認は行っていません。

表 14-2　クライアントレス SSL VPN リモート システム コンフィギュレーションとエンド ユーザの要件 （続き）

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
電子メール プロキシ を介した電子メールの使用	インストール済みの SSL 対応メール アプリケーション ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。	サポートされているメール アプリケーションは次のとおりです。 • Microsoft Outlook • Microsoft Outlook Express バージョン 5.5 および 6.0 その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。
	設定済みのメール アプリケーション	

クライアントレス SSL VPN データのキャプチャ

CLI capture コマンドを使用すると、クライアントレス SSL VPN 接続では正しく表示されない Web サイトに関する情報を記録できます。このデータは、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。次の各項では、キャプチャ コマンドの使用方法について説明します。

- 「キャプチャ ファイルの作成」
- 「キャプチャ データを表示するためのブラウザの使用」

（注） クライアントレス SSL VPN キャプチャをイネーブルにすると、ASA のパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、キャプチャを必ずオフに切り替えます。

キャプチャ ファイルの作成

手順

ステップ 1　クライアントレス SSL VPN キャプチャ ユーティリティを開始してパケットをキャプチャします。

capture *capture-name* **type webvpn user** *csslvpn-username*

例：

```
hostname# capture hr type webvpn user user2
```

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *csslvpn-username* は、キャプチャの対象となるユーザ名です。

ステップ 2　コマンドの **no** バージョンを使用してキャプチャを停止します。

no capture *capture-name*

例：

```
hostname# no capture hr
```

キャプチャ ユーティリティは *capture-name*.zip ファイルを作成し、このファイルはパスワード **koleso** で暗号化されます。

ステップ 3　.zip ファイルをシスコに送信するか、Cisco TAC サービス リクエストに添付します。

ステップ 4　.zip ファイルの内容を確認するには、パスワード **koleso** を使用してファイルを解凍します。

キャプチャ データを表示するためのブラウザの使用

手順

ステップ 1　クライアントレス SSL VPN キャプチャ ユーティリティを開始します。

capture *capture-name* **type webvpn user** *csslvpn-username*

例：

```
hostname# capture hr type webvpn user user2
```

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *csslvpn-username* は、キャプチャの対象となるユーザ名です。

ステップ 2　ブラウザを開き、[Address] ボックスに次のように入力します。

https://*IP address or hostname of the ASA*/**webvpn_capture.html**

キャプチャされたコンテンツが sniffer 形式で表示されます。

ステップ 3　コマンドの **no** バージョンを使用してキャプチャを停止します。

no capture *capture-name*

例：

```
hostname# no capture hr
```

CHAPTER 15

クライアントレス SSL VPN ユーザ

概要

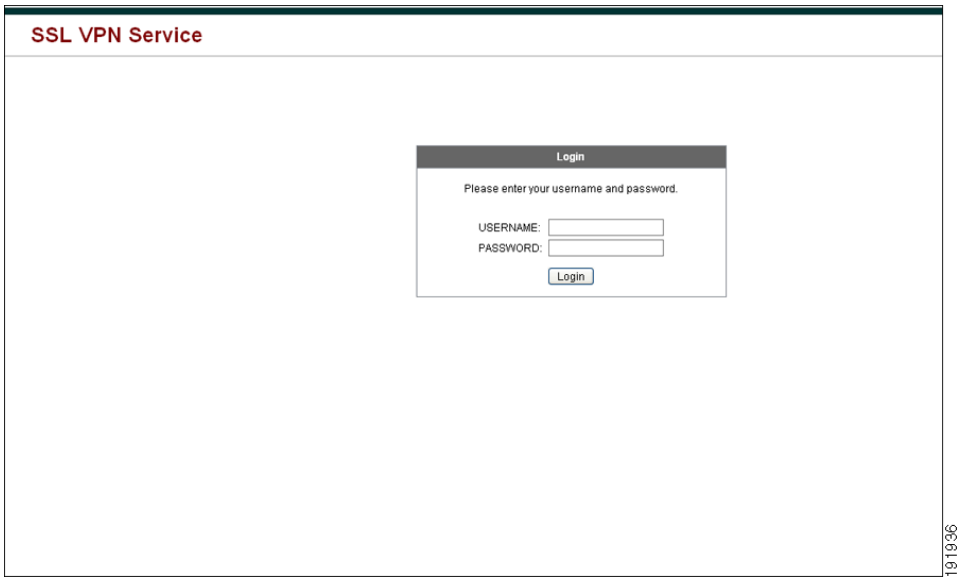
この項では、ユーザがクライアントレス SSL VPN の使用を開始するために、ユーザに伝える必要のある情報を明確にします。説明する項目は次のとおりです。

- 「パスワードの管理」（P.15-3）
- 「自動サインオンの使用」（P.15-9）
- 「セキュリティのヒントの通知」（P.15-11）
- 「クライアントレス SSL VPN の機能を使用するためのリモート システムの設定」（P.15-12）

エンド ユーザ インターフェイスの定義

クライアントレス SSL VPN エンド ユーザ インターフェイスは一連の HTML パネルで構成されます。ユーザは、ASA インターフェイスの IP アドレスを https://*address* 形式で入力することにより、クライアントレス SSL VPN にログインします。最初に表示されるパネルは、ログイン画面（図 15-1）です。

図 15-1　クライアントレス SSL VPN の [Login] 画面



クライアントレス SSL VPN ホーム ページの表示

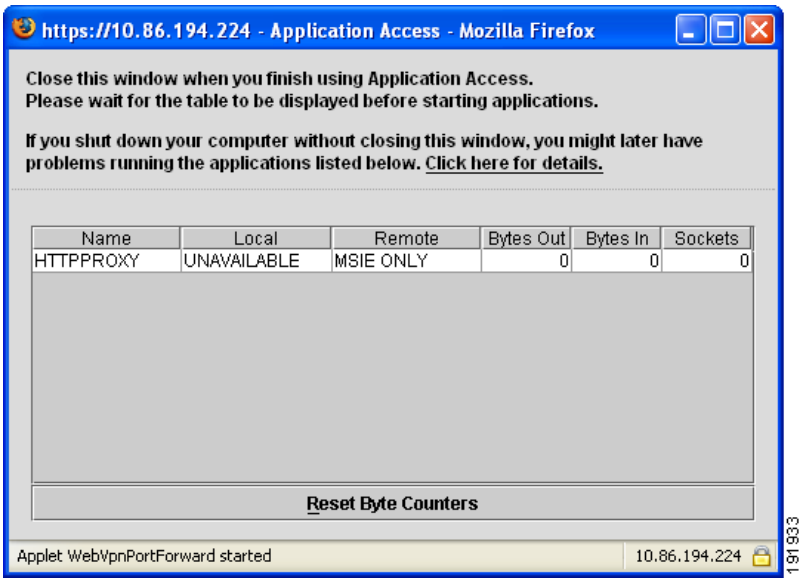
ユーザがログインすると、ポータル ページが開きます。

ホーム ページには設定済みのクライアントレス SSL VPN 機能がすべて表示され、選択済みのロゴ、テキスト、および色が外観に反映されています。このサンプル ホーム ページには、特定のファイル共有の指定機能以外のすべてのクライアントレス SSL VPN 機能が表示されています。ユーザはこのホーム ページを使用して、ネットワークのブラウズ、URL の入力、特定の Web サイトへのアクセス、および Application Access（ポート転送とスマート トンネル）による TCP アプリケーションへのアクセスを実行できます。

クライアントレス SSL VPN の Application Access パネルの表示

ポート転送またはスマート トンネルを開始するには、[Application Access] ボックスの [Go] ボタンをクリックします。[Application Access] ウィンドウが開きます（図 15-2）。

図 15-2　クライアントレス SSL VPN の [Application Access] ウィンドウ



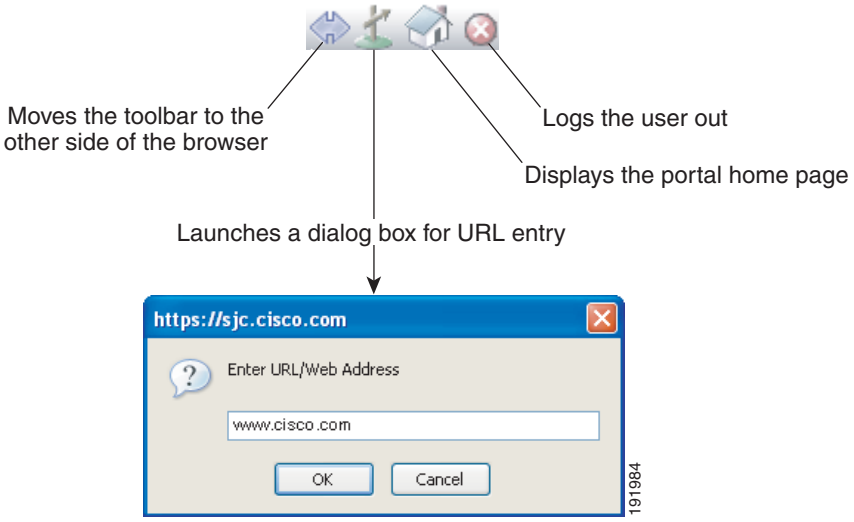
このウィンドウには、このクライアントレス SSL VPN 接続用に設定された TCP アプリケーションが表示されます。このパネルを開いたままでアプリケーションを使用する場合は、通常の方法でアプリケーションを起動します。

（注）　ステートフル フェールオーバーでは、Application Access を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。

フローティング ツールバーの表示

図 15-3 に示すフローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。

図 15-3　クライアントレス SSL VPN フローティング ツールバー



フローティング ツールバーの次の特性に注意してください。

- ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。
- ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。
- ツールバーを閉じると、ASA はクライアントレス SSL VPN セッションを終了するよう促すメッセージを表示します。

クライアントレス SSL VPN の使用方法については、表 15-1（P.15-11）を参照してください。

パスワードの管理

オプションで、パスワードの期限切れが近づくとエンド ユーザに警告するように ASA を設定できます。

ASA では、RADIUS および LDAP プロトコルのパスワード管理をサポートします。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPsec リモート アクセスと SSL VPN トンネル グループのパスワード管理を設定できます。パスワード管理を設定すると、ASA は、リモート ユーザのログイン時に、現在のパスワードの期限切れが近づいていること、または期限が切れていることを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このコマンドは、そのような通知をサポートする AAA サーバに対して有効です。

ASA のリリース 7.1 以降では通常、LDAP による認証時、または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

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

RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバのみに対して通信しているように見えます。

前提条件

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

  認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

  Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
  Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。制約事項
- MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。
- Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポート *されません*。
- LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。
- RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

手順の詳細

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] > [Add or Edit] > [Advanced] > [General] > [Password Management] に移動します。

ステップ 2　[Enable password management] オプションをクリックします。

シスコの認証スキームの SiteMinder への追加

SiteMinder による SSO を使用するための ASA の設定に加え、Java プラグインとして提供されているシスコの認証スキーム（シスコの Web サイトからダウンロード）を使用するようにユーザの CA SiteMinder ポリシー サーバを設定する必要もあります。

前提条件

SiteMinder ポリシー サーバを設定するには、SiteMinder の経験が必要です。

手順の詳細

この項では、手順のすべてではなく、一般的なタスクを取り上げます。

ステップ 1　SiteMinder Administration ユーティリティを使用して、次の特定の引数を使用できるようにカスタム認証スキームを作成します。

- [Library] フィールドに、**smjavaapi** と入力します。
- [Secret] フィールドに、ASA に設定したものと同じ秘密キーを入力します。

  コマンドライン インターフェイスで **policy-server-secret** コマンドを使用して、ASA に秘密キーを設定します。
- [Parameter] フィールドに、**CiscoAuthAPI** と入力します。

ステップ 2　Cisco.com にログインして、http://www.cisco.com/cisco/software/navigator.html から **cisco_vpn_auth.jar** ファイルをダウンロードして、SiteMinder サーバのデフォルトのライブラリ ディレクトリにコピーします。この .jar ファイルは、Cisco ASA CD にも含まれています。

SAML POST SSO サーバの設定

サーバ ソフトウェア ベンダーが提供する SAML サーバのマニュアルに従って、SAML サーバを Relying Party モードで設定します。

手順の詳細

ステップ 1　アサーティング パーティ（ASA）を表す SAML サーバ パラメータを設定します。

- Recipient consumer URL（ASA で設定する assertion consumer URL と同一）
- Issuer ID（通常はアプライアンスのホスト名である文字列）
- Profile type：Browser Post Profile

ステップ 2　証明書を設定します。

ステップ 3　アサーティング パーティのアサーションには署名が必要なことを指定します。

ステップ 4　SAML サーバがユーザを特定する方法を、次のように選択します。

- Subject Name Type が DN
- Subject Name format が uid=<user>

HTTP Form プロトコルを使用した SSO の設定

この項では、SSO における HTTP Form プロトコルの使用について説明します。HTTP Form プロトコルは、SSO 認証を実行するための手段で、AAA 方式としても使用できます。このプロトコルは、クライアントレス SSL VPN のユーザおよび認証を行う Web サーバの間で認証情報を交換するセキュアな方法を提供します。RADIUS サーバや LDAP サーバなどの他の AAA サーバと組み合わせて使用することができます。

前提条件

HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

制約事項

これは、一般的なプロトコルとして、認証に使用する Web サーバ アプリケーションの次の条件に一致する場合にだけ適用できます。

- 認証クッキーは、正常な要求に対して設定され、未許可のログインに対して設定されないようにする必要があります。この場合、ASA は、成功した認証と失敗した認証を区別することはできません。

手順の詳細

ASA は、ここでも認証 Web サーバに対するクライアントレス SSL VPN のユーザのプロキシとして機能しますが、この場合は、要求に対して HTTP Form プロトコルと POST 方式を使用します。フォーム データを送受信するように ASA を設定する必要があります。図 15-4 は、次の SSO 認証手順を示しています。

ステップ 1　最初に、クライアントレス SSL VPN のユーザは、ユーザ名とパスワードを入力して ASA 上のクライアントレス SSL VPN サーバにログオンします。

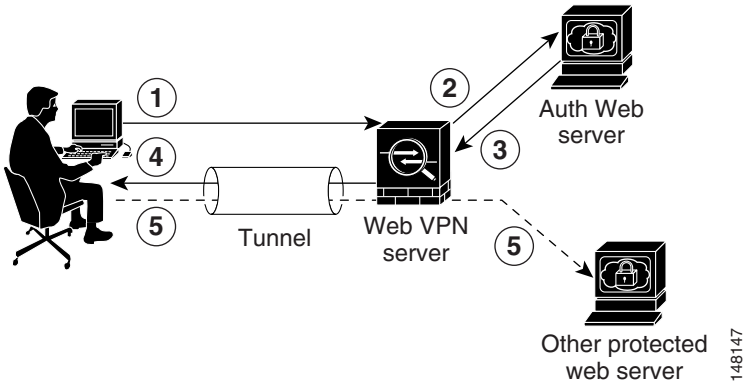
ステップ 2　ユーザのプロキシとして動作するクライアントレス SSL VPN サーバは、このフォーム データ（ユーザ名およびパスワード）を、POST 認証要求を使用して認証する Web サーバに転送します。

ステップ 3　認証する Web サーバがユーザのデータを承認した場合は、認証クッキーをユーザの代行で保存していたクライアントレス SSL VPN サーバに戻します。

ステップ 4　クライアントレス SSL VPN サーバはユーザまでのトンネルを確立します。

ステップ 5　これでユーザは、ユーザ名やパスワードを再入力しなくても、保護された SSO 環境内の他の Web サイトにアクセスできるようになります。

図 15-4　HTTP Form を使用した SSO 認証



ASA でユーザ名やパスワードなどの POST データを含めるようにフォーム パラメータを設定しても、Web サーバが要求する非表示のパラメータが追加されたことに、ユーザが最初に気付かない可能性があります。認証アプリケーションの中には、ユーザ側に表示されず、ユーザが入力することもない非表示データを要求するものもあります。ただし、認証 Web サーバが要求する非表示パラメータを見つけるのは可能です。これは、ASA を仲介役のプロキシとして使用せずに、ユーザのブラウザから Web サーバに直接認証要求を出す方法で行います。HTTP ヘッダー アナライザを使用して Web サーバの応答を分析すると、非表示パラメータが次のような形式で表示されます。

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

非表示パラメータには、必須のパラメータとオプションのパラメータとがあります。Web サーバが非表示パラメータのデータを要求すると、Web サーバはそのデータを省略するすべての認証 POST 要求を拒否します。ヘッダー アナライザは、非表示パラメータが必須かオプションかについては伝えないため、必須のパラメータが判別できるまではすべての非表示パラメータを含めておくことをお勧めします。

HTTP Form データの収集

この項では、必要な HTTP Form データを検出および収集する手順を示します。認証 Web サーバが要求するパラメータが何かわからない場合は、認証交換を分析するとパラメータ データを収集することができます。

前提条件

これらの手順では、ブラウザと HTTP ヘッダー アナライザが必要です。

手順の詳細

ステップ 1　ユーザのブラウザと HTTP ヘッダー アナライザを起動して、ASA を経由せずに Web サーバのログイン ページに直接接続します。

ステップ 2　Web サーバのログイン ページがユーザのブラウザにロードされてから、ログイン シーケンスを検証して交換時にクッキーが設定されているかどうか判別します。Web サーバによってログイン ページにクッキーがロードされている場合は、このログイン ページの URL を *start-URL* として設定します。

ステップ 3　Web サーバにログオンするためのユーザ名とパスワードを入力して、Enter を押します。この動作によって、ユーザが検証する認証 POST 要求が HTTP ヘッダー アナライザを使用して生成されます。

次に、ホストの HTTP ヘッダーおよび本文が記載された POST 要求の例を示します。

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05
-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIr
NT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmye
mco%2FHTTP/1.1

Host: www.example.com

(BODY)

SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%
2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

ステップ 4　POST 要求を検証してプロトコル、ホストをコピーし、URL を入力して action-uri パラメータを設定します。

ステップ 5　POST 要求の本文を検証して、次の情報をコピーします。

a. ユーザ名パラメータ。上記の例では、このパラメータは *USERID* で、値 *anyuser* ではありません。

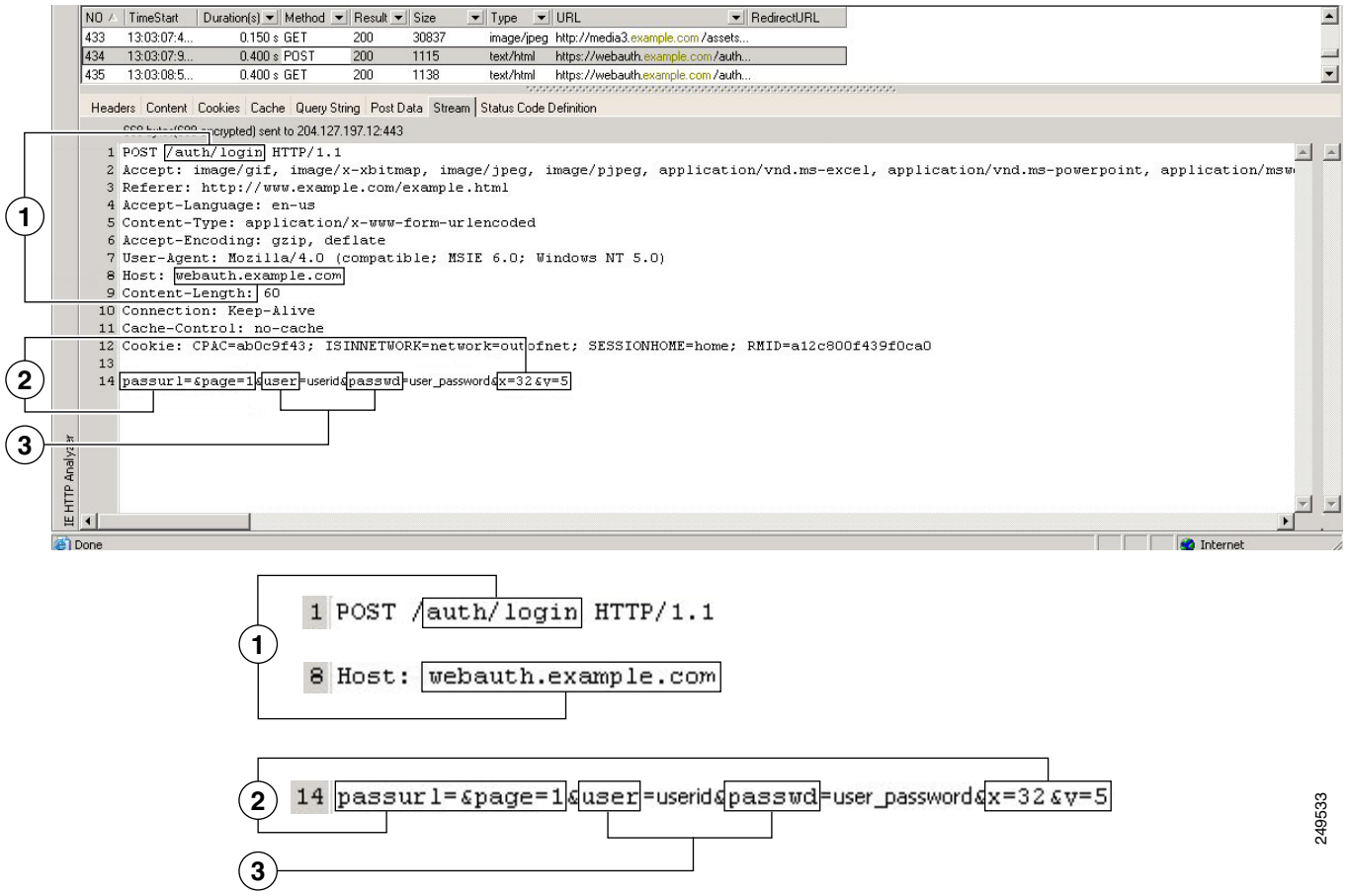
b. パスワード パラメータ。上記の例では、このパラメータは *USER_PASSWORD* です。

c. 非表示パラメータ。このパラメータは、POST 本文からユーザ名パラメータとパスワード パラメータを除くすべてです。前の例の非表示パラメータは次のとおりです。

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0

図 15-5 は、HTTP アナライザの出力例に表示される action URI、非表示、ユーザ名、パスワードの各種パラメータを強調して示したものです。これは一例です。出力は Web サイトによって大幅に異なることがあります。

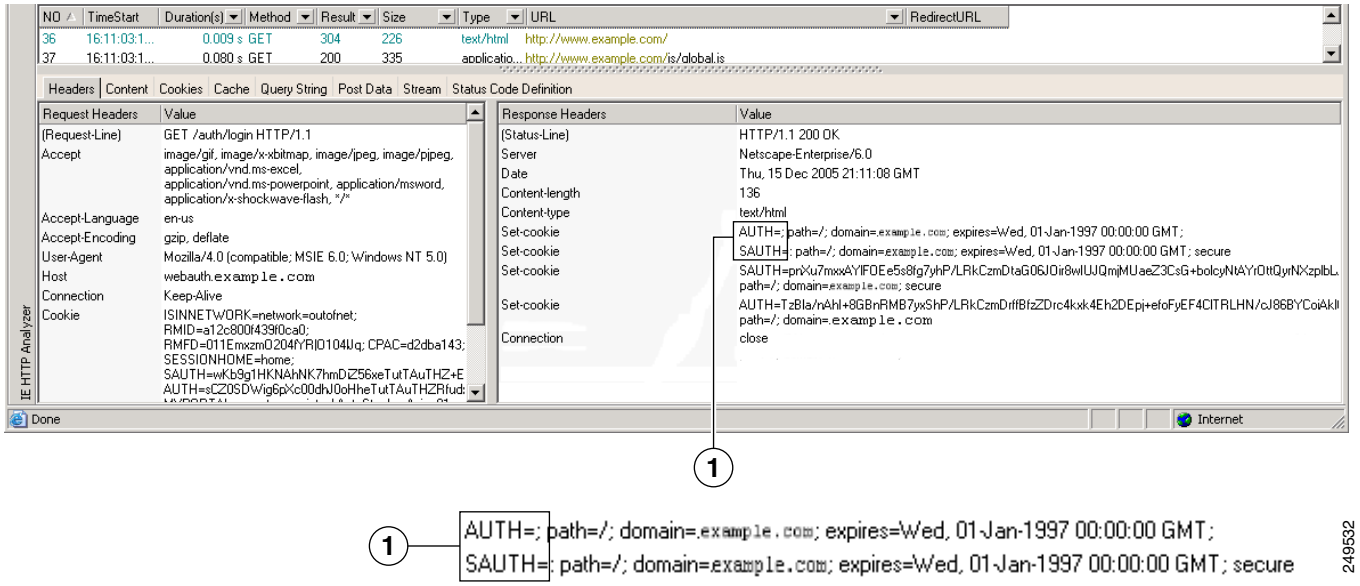
図 15-5　action-uri、非表示、ユーザ名、パスワードの各種パラメータ



ステップ 6　Web サーバへのログオンが成功したら、HTTP ヘッダー アナライザを使用して、サーバからユーザのブラウザに設定されているクッキー名を見つけ出すことによって、サーバの応答を検証します。これは **auth-cookie-name** パラメータです。

次のサーバ応答ヘッダーでは、SMSESSION がセッションのクッキーの名前です。必要なのはこの名前だけです。値は不要です。図 15-6 に、HTTP アナライザによる認可クッキーの出力例を示します。これは一例です。出力は Web サイトによって大幅に異なることがあります。

図 15-6　　HTTP アナライザの出力例に表示された認可クッキー



1	認可クッキー

ステップ 7　場合によっては、認証の成否にかかわらず同じクッキーがサーバによって設定される可能性があり、このようなクッキーは、SSO の目的上、認められません。クッキーが異なっていることを確認するには、無効なログイン クレデンシャルを使用してステップ 1 からステップ 6 を繰り返し、「失敗」クッキーと「成功した」クッキーとを比較します。これで、HTTP Form プロトコルによる SSO を ASA に設定するために必要なパラメータ データを入手できました。

自動サインオンの使用

[Auto Sign-on] ウィンドウまたはタブでは、クライアントレス SSL VPN ユーザの自動サインオンを設定または編集できます。自動サインオンは、内部ネットワークに SSO 方式をまだ展開していない場合に使用できる簡素化された単一サインオン方式です。特定の内部サーバに対して自動サインオンを設定すると、ASA は、クライアントレス SSL VPN ユーザが ASA へのログオンで入力したログイン クレデンシャル（ユーザ名とパスワード）をそれら特定の内部サーバに渡します。特定の範囲のサーバの特定の認証方式に応答するように、ASA を設定します。ASA が応答するように設定可能な認証方式は、Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべてを使用する認証で構成されます。

ユーザ名とパスワードのルックアップが ASA で失敗した場合は、空の文字列で置き換えられ、動作は自動サインオンが不可の場合の状態に戻されます。

自動サインオンは、特定の内部サーバに SSO を設定する直接的な方法です。この項では、自動サインオンを行うように SSO をセットアップする手順について説明します。Computer Associates SiteMinder SSO サーバを使用して SSO をすでに導入している場合、または Security Assertion Markup Language（SAML）Browser Post Profile SSO がある場合。このソリューションをサポートするように ASA を設定するには、「SSO サーバ」（P.12-7）を参照してください。

次のフィールドが表示されます。

- [IP Address]：次の [Mask] と組み合わせて、認証されるサーバの IP アドレスの範囲を [Add/Edit Auto Sign-on] ダイアログボックスで設定されたとおりに表示します。サーバは、サーバの URI またはサーバの IP アドレスとマスクで指定できます。
- [Mask]：前の [IP Address] と組み合わせて、[Add/Edit Auto Sign-on] ダイアログボックスで自動サインオンをサポートするように設定されたサーバの IP アドレスの範囲を表示します。
- [URI]：[Add/Edit Auto Sign-on] ダイアログボックスで設定されたサーバを識別する URI マスクを表示します。
- [Authentication Type]：[Add/Edit Auto Sign-on] ダイアログボックスで設定された認証のタイプ（Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべて）を表示します。

制約事項

- 認証が不要なサーバ、または ASA とは異なるクレデンシャルを使用するサーバでは、自動サインオンをイネーブルにしないでください。自動サインオンがイネーブルの場合、ASA は、ユーザ ストレージにあるクレデンシャルに関係なく、ユーザが ASA へのログオンで入力したログイン クレデンシャルを渡します。
- 一定範囲のサーバに対して 1 つの方式（HTTP Basic など）を設定する場合に、その中の 1 台のサーバが異なる方式（NTLM など）で認証を試みると、ASA はユーザのログイン クレデンシャルをそのサーバに渡しません。

手順の詳細

ステップ 1　クリックして自動サインオン命令を追加または編集します。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。

ステップ 2　[Auto Sign-on] テーブルで選択した自動サインオン命令を削除する場合にクリックします。

ステップ 3　[IP Block] をクリックして、IP アドレスとマスクを使用して内部サーバの範囲を指定します。

- [IP Address]：自動サインオンを設定する範囲の最初のサーバの IP アドレスを入力します。
- [Mask]：[subnet mask] メニューで、自動サインオンをサポートするサーバのサーバ アドレス範囲を定義するサブネット マスクを選択します。

ステップ 4　[URI] をクリックして、URI によって自動サインオンをサポートするサーバを指定し、このボタンの横にあるフィールドに URI を入力します。

ステップ 5　サーバに割り当てられる認証方式を決定します。指定された範囲のサーバの場合には、Basic HTTP 認証要求、NTLM 認証要求、FTP と CIFS の認証要求、またはこれら方式のいずれかを使用する要求に応答するように、ASA を設定できます。

- [Basic]：サーバが Basic（HTTP）認証をサポートする場合は、このボタンをクリックします。
- [NTLM]：サーバが NTLMv1 認証をサポートする場合は、このボタンをクリックします。
- [FTP/CIFS]：サーバが FTP と CIFS の認証をサポートする場合は、このボタンをクリックします。
- [Basic, NTLM, and FTP/CIFS]：サーバが上のすべての方式をサポートする場合は、このボタンをクリックします。

ユーザ名とパスワードの要求

ネットワークによっては、リモート セッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、クライアントレス SSL VPN、メール サーバ、ファイル サーバ、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。

表 15-1 に、クライアントレス SSL VPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 15-1　クライアントレス SSL VPN セッションのユーザに提供するユーザ名とパスワード

ログイン ユーザ名/パスワード タイプ	目的	入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN の起動
ファイル サーバ	リモート ファイル サーバへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	クライアントレス SSL VPN 経由によるリモート メール サーバへのアクセス	電子メール メッセージの送受信

セキュリティのヒントの通知

ユーザはいつでもツールバーの [Logout] アイコンをクリックして、クライアントレス SSL VPN セッションを閉じることができます（ブラウザ ウィンドウを閉じてもセッションは閉じません）。

クライアントレス SSL VPN は、企業ネットワーク上のリモート PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。クライアントレス SSL VPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信は暗号化されていないため、プライベートではありません。

「クライアントレス SSL VPN セキュリティ対策」（P.1）に、セッション内で実行する手順に応じて、ユーザと通信するための追加のヒントを示します。

クライアントレス SSL VPN の機能を使用するためのリモート システムの設定

この項では、クライアントレス SSL VPN を使用するようにリモート システムを設定する方法について説明します。

ユーザ アカウントを別々に設定でき、各ユーザは異なるクライアントレス SSL VPN の機能を使用できます。

クライアントレス SSL VPN の起動

次のようなサポートされている接続を使用して、インターネットに接続できます。

- 家庭の DSL、ケーブル、ダイヤルアップ。
- 公共のキオスク。
- ホテルのホットスポット。
- 空港の無線ノード。
- インターネット カフェ。

（注）　クライアントレス SSL VPN がサポートする Web ブラウザのリストについては、『*Supported VPN Platforms, Cisco ASA Series*』を参照してください。

前提条件

- ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
- クライアントレス SSL VPN の URL が必要です。URL は、https://*address* の形式の https アドレスである必要があります。*address* は、SSL VPN がイネーブルである ASA（またはロードバランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、https://cisco.example.com などです。
- クライアントレス SSL VPN のユーザ名とパスワードが必要です。

制約事項

- クライアントレス SSL VPN ではローカル印刷がサポートされていますが、VPN 経由による企業ネットワーク上のプリンタへの印刷はサポートされていません。

クライアントレス SSL VPN フローティング ツールバーの使用

フローティング ツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。

フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。[Close] ボタンをクリックすると、ASA によってクライアントレス SSL VPN セッションを閉じることを求めるメッセージが表示されます。

ヒント テキストをテキスト フィールドに貼り付けるには、Ctrl を押した状態で V を押します（クライアントレス SSL VPN セッション中は、表示されるツールバー上での右クリックはオフになっています）。

制約事項

ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。

Web のブラウズ

クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。「セキュリティのヒントの通知」を参照してください。

クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。

- クライアントレス SSL VPN のタイトル バーが各 Web ページの上部に表示される。
- Web サイトへのアクセス方法：
  - クライアントレス SSL VPN [Home] ページ上の [Enter Web Address] フィールドに URL を入力する
  - クライアントレス SSL VPN [Home] ページ上にある設定済みの Web サイト リンクをクリックする
  - 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN [Home] ページ上にリンクとして表示されるものに限られる

前提条件

保護されている Web サイトのユーザ名とパスワードが必要です。

制約事項

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN [Home] ページ上にリンクとして表示されるものに限られる

ネットワークのブラウズ（ファイル管理）

ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。

（注）　コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。

前提条件

- 共有リモート アクセス用にファイル アクセス権を設定する必要があります。
- 保護されているファイル サーバのサーバ名とパスワードが必要です。
- フォルダとファイルが存在するドメイン、ワークグループ、およびサーバの名前が必要です。

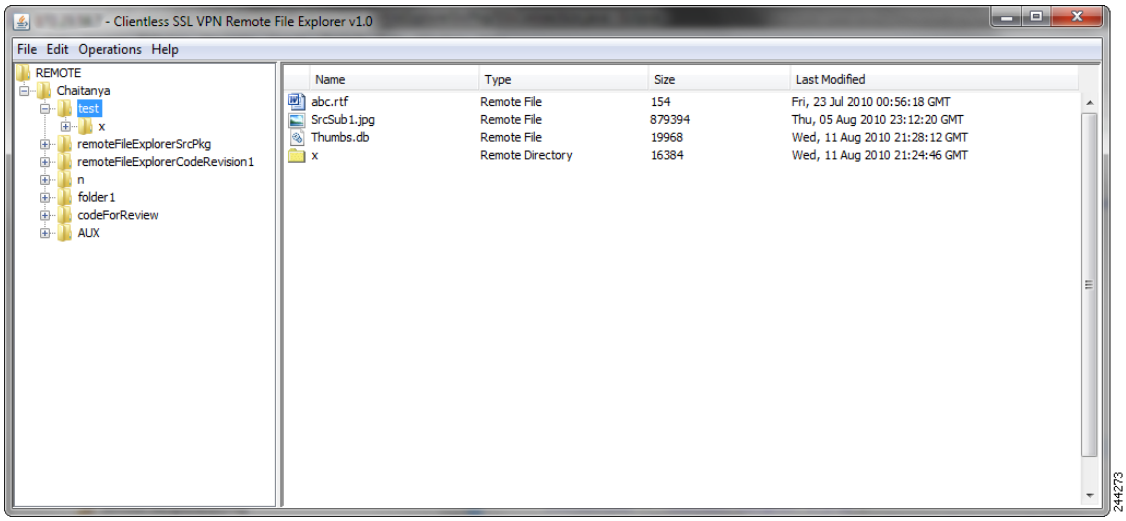
制約事項

クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。

Remote File Explorer の使用

ユーザは、Remote File Explorer を使用して、Web ブラウザから企業ネットワークをブラウズできます。ユーザが Cisco SSL VPN ポータル ページの [Remote File System] アイコンをクリックすると、ユーザのシステムでアプレットが起動し、ツリーおよびフォルダ ビューにリモート ファイル システムが表示されます。

図 15-7　Clientless SSL VPN Remote File Explorer



ユーザはブラウザで次を実行できます。

- リモート ファイル システムのブラウズ。
- ファイルの名前の変更。
- リモート ファイル システム内、およびリモートとローカルのファイル システム間でのファイルの移動またはコピー
- ファイルのバルク アップロードおよびダウンロードの実行。

（注） この機能では、ユーザのマシンに Oracle Java ランタイム環境（JRE）1.4 以降がインストールされ、Web ブラウザで Java がイネーブルになっている必要があります。リモート ファイルの起動には、JRE 1.6 以降が必要です。

ファイルまたはフォルダの名前変更

ファイルまたはフォルダの名前を変更するには、次の手順を実行します。

ステップ 1　名前を変更するファイルまたはフォルダをクリックします。

ステップ 2　[Edit] > [Rename] を選択します。

ステップ 3　プロンプトが表示されたら、ダイアログに新しい名前を入力します。

ステップ 4　[OK] をクリックして、ファイルまたはフォルダの名前を変更します。または、名前を変更しない場合は [Cancel] をクリックします。

リモート サーバでのファイルやフォルダの移動またはコピー

リモート サーバでファイルやフォルダを移動またはコピーするには、次の手順を実行します。

ステップ 1　移動またはコピーするファイルやフォルダが含まれている送信元フォルダに移動します。

ステップ 2　ファイルまたはフォルダをクリックします。

ステップ 3　ファイルをコピーするには、[Edit] > [Copy] を選択します。また、ファイルを移動するには、[Edit] > [Cut] を選択します。

ステップ 4　宛先フォルダに移動します。

ステップ 5　[Edit] > [Paste] を選択します。

ローカル システム ドライブからリモート フォルダへのファイルのコピー

ローカル ファイル システムとリモート ファイル システム間でファイルをコピーするには、リモート ファイル ブラウザの右ペインとローカル ファイル マネージャ アプリケーション間でファイルをドラッグ アンド ドロップします。

ファイルのアップロードおよびダウンロード

ファイルをダウンロードするには、ブラウザでファイルをクリックし、[Operations] > [Download] を選択し、[Save] ダイアログで場所と名前を指定してファイルを保存します。

ファイルをアップロードするには、宛先フォルダをクリックし、[Operations] > [Upload] を選択し、[Open] ダイアログでファイルの場所と名前を指定します。

この機能には次の制限があります。

- ユーザは、アクセスを許可されていないサブフォルダを表示できません。
- ユーザがアクセスを許可されていないファイルは、ブラウザに表示されても移動またはコピーできません。
- ネストされたフォルダの最大の深さは 32 です。
- ツリー ビューでは、ドラッグ アンド ドロップのコピーがサポートされていません。
- Remote File Explorer の複数のインスタンスの間でファイルを移動するときは、すべてのインスタンスが同じサーバを探索する必要があります（ルート共有）。
- Remote File Explorer は、1 つのフォルダに最大 1500 のファイルおよびフォルダを表示できます。フォルダがこの制限を超えた場合、フォルダは表示されません。

ポート転送の使用

（注）　ユーザは、アプリケーションを使用し終えたら、[Close] アイコンをクリックして必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がオフに切り替わる可能性があります。詳細については、「Application Access 使用時の hosts ファイル エラーからの回復」（P.18-1）を参照してください。

前提条件

- Mac OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。
- クライアント アプリケーションがインストールされている必要があります。
- ブラウザでクッキーをイネーブルにする必要があります。
- DNS 名を使用してサーバを指定する場合、ホスト ファイルの変更に必要になるため、PC に対する管理者アクセス権が必要です。
- Oracle Java ランタイム環境（JRE）バージョン 1.4.x と 1.5.x がインストールされている必要があります。

  JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。まれに、Java 例外エラーで、ポート転送アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。

  a. ブラウザのキャッシュをクリアして、ブラウザを閉じます。
  b. Java アイコンがコンピュータのタスク バーに表示されていないことを確認します。
  c. Java のインスタンスをすべて閉じます。
  d. クライアントレス SSL VPN セッションを確立し、ポート転送 Java アプレットを起動します。
- ブラウザで javascript をイネーブルにする必要があります。デフォルトでは有効に設定されています。
- 必要に応じて、クライアント アプリケーションを設定する必要があります。

（注）　Microsoft Outlook クライアントの場合、この設定手順は不要です。Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] フィールドの値をチェックします。[Remote Server] フィールドにサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。[Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。

制約事項

この機能を使用するには、Oracle Java ランタイム環境（JRE）をインストールしてローカル クライアントを設定する必要があります。これには、ローカル システムでの管理者の許可、または C:\windows\System32\drivers\etc の完全な制御が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

手順の詳細

クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。

1. クライアントレス SSL VPN セッションを開始して、[Home] ページの [Application Access] リンクをクリックします。[Application Access] ウィンドウが表示されます。
2. [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。
3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。

（注）　クライアントレス SSL VPN セッション上で実行しているアプリケーションで URL（電子メール メッセージ内のものなど）をクリックしても、サイトがそのセッションで開くわけではありません。サイトをセッション上で開くには、その URL を [Enter Clientless SSL VPN (URL) Address] フィールドに貼り付けます。

ポート転送を介した電子メールの使用

電子メールを使用するには、クライアントレス SSL VPN のホーム ページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。

（注）　IMAP クライアントの使用中にメール サーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。

前提条件

アプリケーション アクセスおよびその他のメール クライアントの要件を満たしている必要があります。

制約事項

Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。

クライアントレス SSL VPN は、Lotus Notes および Eudora などの、ポート転送を介したその他の SMTPS、POP3S、または IMAP4S 電子メール プログラムをサポートしますが、動作確認は行っていません。

Web アクセスを介した電子メールの使用

次の電子メール アプリケーションがサポートされています。

- Microsoft Outlook Web App to Exchange Server 2010

  OWA には、Internet Explorer 7 以降、または Firefox 3.01 以降が必要です。
- Microsoft Outlook Web Access to Exchange Server 2007、2003、および 2000

  最適な結果を得るために、Internet Explorer 8.x 以降または Firefox 8.x で OWA を使用してください。
- Louts iNotes

前提条件

Web ベースの電子メール製品がインストールされている必要があります。

制約事項

その他の Web ベースの電子メール アプリケーションも動作しますが、動作確認は行っていません。

電子メール プロキシを介した電子メールの使用

次のレガシー電子メール アプリケーションがサポートされています。

- Microsoft Outlook 2000 および 2002
- Microsoft Outlook Express 5.5 および 6.0

メール アプリケーションの使用方法と例については、「クライアントレス SSL VPN を介した電子メールの使用」（P.12-23）を参照してください。

前提条件

- SSL 対応メール アプリケーションがインストールされている必要があります。
- ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。
- メール アプリケーションが正しく設定されている必要があります。

制約事項

その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。

スマート トンネルの使用

スマート トンネルの使用に管理権限は必要ありません。

（注）　ポート フォワーダの場合と異なり、Java は自動的にダウンロードされません。

前提条件

- スマート トンネルには、Windows では ActiveX または JRE（1.4x および 1.5x）、Mac OS X では Java Web Start が必要です。
- ブラウザで Cookie をイネーブルにする必要があります。
- ブラウザで javascript をイネーブルにする必要があります。

制約事項

- Mac OS X では、フロントサイド プロキシはサポートされていません。
- 「スマート トンネル アクセスの設定」（P.13-1）で指定されているオペレーティング システムおよびブラウザだけがサポートされています。
- TCP ソケットベースのアプリケーションだけがサポートされています。

モバイル デバイスでのクライアントレス SSL VPN

モバイル デバイスでのクライアントレス SSL VPN の使用

Pocket PC または他の認定されたモバイル デバイスからクライアントレス SSL VPN にアクセスできます。認定されたモバイル デバイスでクライアントレスの SSL VPN を使用するために、ASA 管理者またはクライアントレス SSL VPN ユーザは特別なことを行う必要はありません。

シスコは、次のモバイル デバイス プラットフォームを認定しています。

HP iPaq H4150

Pocket PC 2003

Windows CE 4.20.0, build 14053

Pocket Internet Explorer (PIE)

ROM version 1.10.03ENG

ROM Date: 7/16/2004

クライアントレス SSL VPN のモバイル デバイスのバージョンによって、次のような相違点があります。

- ポップアップのクライアントレス SSL VPN ウィンドウはバナー Web ページに置き換わっています。
- 標準のクライアントレス SSL VPN フローティング ツールバーがアイコン バーに置き換わっています。このバーには、[Go]、[Home]、および [Logout] の各種ボタンが表示されます。
- メインのクライアントレス SSL VPN ポータル ページに [Show Toolbar] アイコンがありません。
- クライアントレス SSL VPN のログアウト時に、警告メッセージで PIE ブラウザを正しく閉じる手順が表示されます。この手順に従わないで通常の方法でブラウザのウィンドウを閉じると、クライアントレス SSL VPN または HTTPS を使用するすべてのセキュアな Web サイトから PIE が切断されません。

制約事項

- クライアントレス SSL VPN は、OWA 2000 版および OWA 2003 版の基本認証をサポートしています。OWA サーバに基本認証を設定せずにクライアントレス SSL VPN ユーザがこのサーバにアクセスしようとするとアクセスは拒否されます。
- サポートされていないクライアントレス SSL VPN の機能
  - Application Access および他の Java 依存の各種機能
  - HTTP プロキシ
  - Citrix Metaframe 機能（PDA に対応する Citrix ICA クライアント ソフトウェアが装備されていない場合）

CHAPTER 17

クライアントレス SSL VPN のカスタマイズ

クライアントレス SSL VPN ユーザ エクスペリエンスのカスタマイズ

ログイン ページ、ポータル ページ、ログアウト ページなどの、クライアントレス SSL VPN ユーザ エクスペリエンスをカスタマイズできます。2 つの方式を使用できます。[Add/Edit Customization Object] ウィンドウで、事前定義されたページ コンポーネントをカスタマイズできます。このウィンドウでは、ページをカスタマイズするために使用される、ASA 上に保存される XML ファイル（カスタマイゼーション オブジェクト）を追加または変更します。または、XML ファイルをローカル コンピュータまたはサーバにエクスポートし、XML タグを変更し、ファイルを ASA に再インポートできます。どちらの方式でも、接続プロファイルまたはグループ ポリシーに適用するカスタマイゼーション オブジェクトが作成されます。

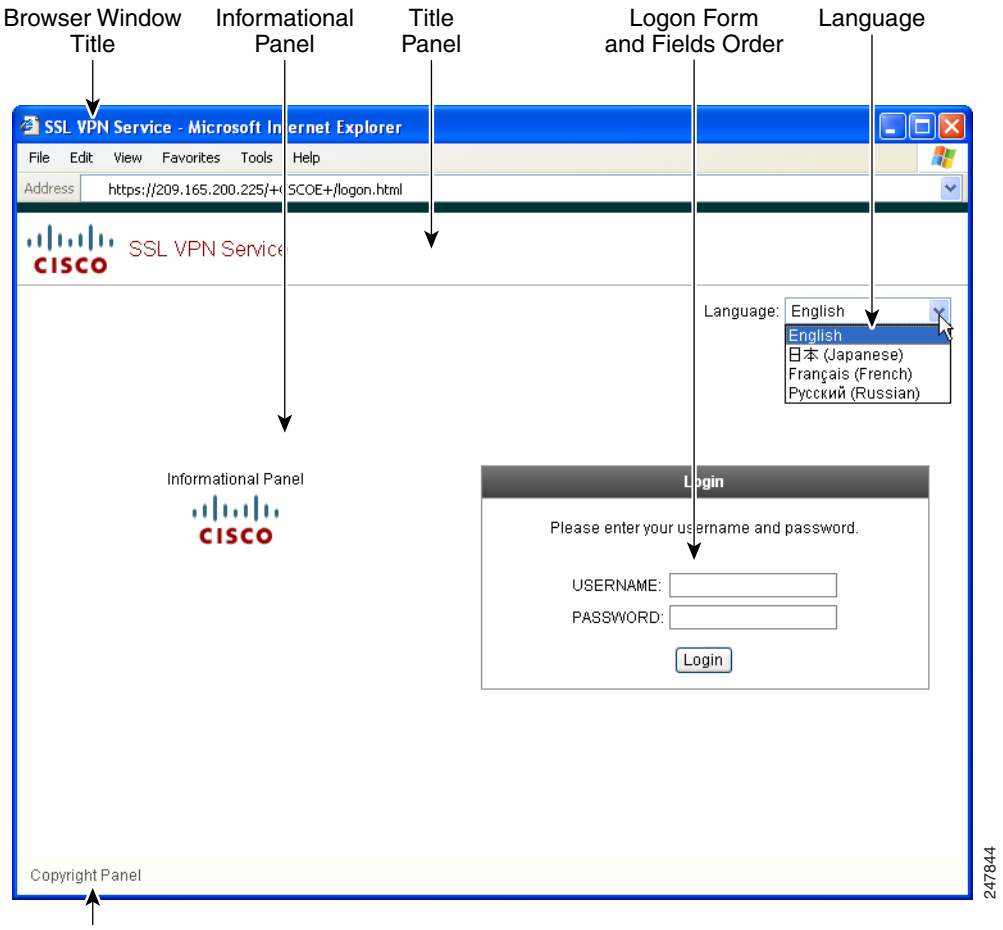
ログイン ページの事前定義されたコンポーネントをカスタマイズするのではなく、独自のページを作成して ASA にインポートできます（フル カスタマイゼーション）。

ログイン ページの事前定義されたコンポーネントをカスタマイズできます。タイトル、言語オプション、ユーザへのメッセージなどがあります。または、独自のカスタム ページでページを完全に置き換えることができます（フル カスタマイゼーション）。

Customization Editor によるログイン ページのカスタマイズ

図 17-1 に、ログイン ページとカスタマイズ可能な事前定義されたコンポーネントを示します。

図 17-1　クライアントレス ログイン ページのコンポーネント



ログイン ページのすべてのコンポーネントをカスタマイズするには、次の手順を実行します。[Preview] ボタンをクリックして、各コンポーネントに対する変更をプレビューできます。

ステップ 1　事前定義されたカスタマイゼーションを指定します。[Logon Page] に移動し、[Customize pre-defined logon page components] を選択します。ブラウザ ウィンドウのタイトルを指定します。

ステップ 2　タイトル パネルを表示し、カスタマイズします。[Logon Page] > [Title Panel] の順に選択し、[Display title panel] をオンにします。タイトルとして表示するテキストを入力し、ロゴを指定します。フォント スタイルを指定します。

ステップ 3　表示する言語オプションを指定します。[Logon Page] > [Language] の順に選択し、[Enable Language Selector] をオンにします。リモート ユーザに表示する言語を追加または削除します。リスト内の言語には、[Configuration] > [Remote Access VPN] > [Language Localization] で設定する変換テーブルが必要です。

ステップ 4　ログイン フォームをカスタマイズします。[Logon Page] > [Logon Form] の順に選択します。フォームのテキストおよびパネル内のフォント スタイルをカスタマイズします。接続プロファイルでセカンダリ認証サーバが設定されている場合にのみ、セカンダリ パスワード フィールドがユーザに表示されます。

ステップ 5　ログイン フォームのフィールドを配置します。[Logon Page] > [Form Fields Order] の順に選択します。上矢印ボタンと下矢印ボタンを使用して、フィールドが表示される順序を変更します。

ステップ 6　ユーザへのメッセージを追加します。[Logon Page] > [Informational Panel] の順に選択し、[Display informational panel] をオンにします。パネルに表示するテキストを追加し、ログイン フォームに対してパネルの位置を変更し、このパネルに表示するロゴを指定します。

ステップ 7　著作権宣言文を表示します。[Logon Page] > [Copyright Panel] の順に選択し、[Display copyright panel] をオンにします。著作権のために表示するテキストを追加します。

ステップ 8　[OK] をクリックしてから、編集したカスタマイゼーション オブジェクトに変更を適用します。

次の作業

独自の完全にカスタマイズしたページでのログイン ページの置き換えについて確認してください。

独自の完全にカスタマイズしたページでのログイン ページの置き換え

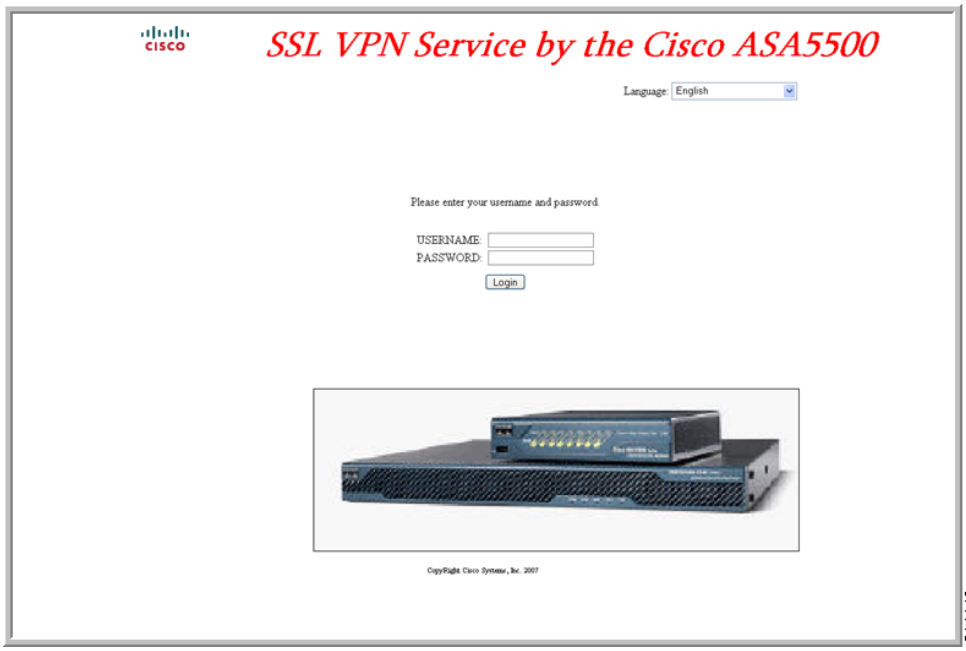
提供されるログイン ページの特定のコンポーネントを変更するのではなく、独自のカスタム ログイン画面を使用する場合は、フル カスタマイゼーション機能を使用してこの高度なカスタマイゼーションを実行できます。

フル カスタマイゼーションを使用して、独自のログイン画面の HTML を入力し、ASA で関数を呼び出す Cisco HTML コードを挿入します。これで、Login フォームと言語セレクタ ドロップダウン リストが作成されます。

このマニュアルでは、独自の HTML コードを作成するために必要な修正内容、および ASA が独自のコードを使用する場合に設定する必要があるタスクについて説明します。

図 17-2 は、フル カスタマイゼーション機能によってイネーブル化される簡単なカスタム ログイン画面の例を示しています。

図 17-2　ログイン ページのフル カスタマイゼーション例



カスタム ログイン画面ファイルの作成

次の HTML コードは例として使用され、表示するコードです。

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font
color="#FF0000" size="7" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font></b></i></p>

    <body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

    <table>

    <tr><td colspan=3 height=20 align=right><div id="selector" style="width:
    300px"></div></td></tr>
    <tr><td></td><td></td><td></td></tr>
    <tr>
    <td height="379"></td>
    <td height="379"></td>
    <td align=middle valign=middle>
    <div id=lform >
    <p> </p>
    <p> </p>
    <p> </p>
    <p>Loading...</p>
    </div>
    </td>
    </tr>
    <tr>
    <td width="251"></td>
    <td width="1"></td>
    <td align=right valign=right width="800">
    <img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
    </td></tr>

    </table>
```

字下げされたコードは、画面に Login フォームと言語セレクタを挿入します。関数 **csco_ShowLoginForm('lform')** は Login フォームを挿入します。**csco_ShowLanguageSelector('selector')** は、言語セレクタを挿入します。

ステップ 1　ファイルに **login.inc** という名前を付けます。このファイルをインポートすると、ASA はこのファイル名をログイン画面として認識します。

ステップ 2　このファイルで使用されるイメージのパスに **/+CSCOU+/** を含めるように変更します。

認証前にリモート ユーザに表示されるファイルは、パス /+CSCOU+/ で表される ASA のキャッシュ メモリの特定のエリアに置く必要があります。そのため、このファイルにある各イメージのソースはこのパスに含める必要があります。次に例を示します。

```
src="/+CSCOU+/asa5520.gif"
```

ステップ 3　下記の特別な HTML コードを挿入します。このコードには、Login フォームと言語セレクタを画面に挿入する前述のシスコの関数が含まれています。

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td><td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

ファイルおよびイメージのインポート

ステップ 1　[Clientless SSL VPN Access] > [Portal] > [Web Contents] の順に選択します。

ステップ 2　[Import] をクリックします。

a.　[Source] オプションを選択し、Web コンテンツをファイルのパスを入力します。

b.　[Destination] 領域で、[Require Authentication to access its content] に対して [No] を選択します。これにより、ファイルは、認証の前にユーザがアクセスできるフラッシュ メモリの領域に保存されます。

ステップ 3　[Import Now] をクリックします。

カスタム ログイン画面を使用するセキュリティ アプライアンスの設定

ステップ 1　[Clientless SSL VPN Access] > [Portal] > [Customization] のテーブルでカスタマイゼーション オブジェクトを選択し、[Edit] をクリックします。

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

ステップ 3　[Replace pre-defined logon page with a custom page] を選択します。

ステップ 4　[Manage] をクリックして、ログイン ページ ファイルをインポートします。

ステップ 5　[Destination] 領域で、[No] を選択して、認証の前にログイン ページがユーザに表示されるようにします。

ステップ 6　[Edit Customization Object] ウィンドウに戻り、[General] をクリックして、必要な接続プロファイルおよびグループ ポリシーのカスタマイゼーション オブジェクトをイネーブルにします。

クライアントレス SSL VPN エンド ユーザの設定

この項は、エンド ユーザのためにクライアントレス SSL VPN を設定するシステム管理者を対象にしています。ここでは、エンド ユーザ インターフェイスをカスタマイズする方法、およびリモート システムの設定要件と作業の概要を説明します。ユーザがクライアントレス SSL VPN の使用を開始するために、ユーザに伝える必要のある情報を明確にします。

エンド ユーザ インターフェイスの定義

クライアントレス SSL VPN エンド ユーザ インターフェイスは一連の HTML パネルで構成されます。ユーザは、ASA インターフェイスの IP アドレスを https://*address* 形式で入力することにより、クライアントレス SSL VPN にログインします。最初に表示されるパネルは、ログイン画面です。

クライアントレス SSL VPN ホーム ページの表示

ユーザがログインすると、ポータル ページが開きます。

ホーム ページには設定済みのクライアントレス SSL VPN 機能がすべて表示され、選択済みのロゴ、テキスト、および色が外観に反映されています。このサンプル ホーム ページには、特定のファイル共有の指定機能以外のすべてのクライアントレス SSL VPN 機能が表示されています。ユーザはこのホーム ページを使用して、ネットワークのブラウズ、URL の入力、特定の Web サイトへのアクセス、および Application Access（ポート転送とスマート トンネル）による TCP アプリケーションへのアクセスを実行できます。

クライアントレス SSL VPN の Application Access パネルの表示

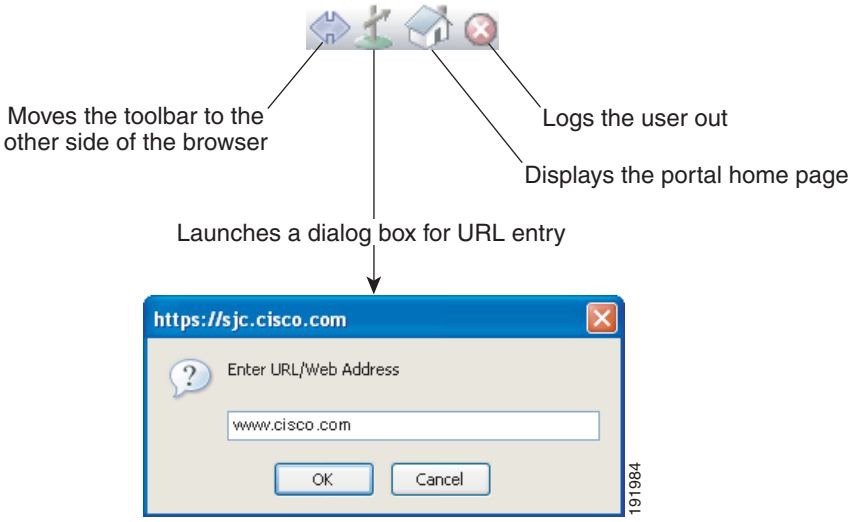
ポート転送またはスマート トンネルを開始するには、[Application Access] ボックスの [Go] ボタンをクリックします。[Application Access] ウィンドウが開き、このクライアントレス SSL VPN 接続用に設定された TCP アプリケーションが表示されます。このパネルを開いたままでアプリケーションを使用する場合は、通常の方法でアプリケーションを起動します。

（注）　ステートフル フェールオーバーでは、Application Access を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。

フローティング ツールバーの表示

図 17-3 に示すフローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。

図 17-3　クライアントレス SSL VPN フローティング ツールバー



フローティング ツールバーの次の特性に注意してください。

- ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。
- ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。
- ツールバーを閉じると、ASA はクライアントレス SSL VPN セッションを終了するよう促すメッセージを表示します。

クライアントレス SSL VPN ページのカスタマイズ

クライアントレス SSL VPN ユーザに表示されるポータル ページの外観を変えることができます。変更できる外観には、ユーザがセキュリティ アプライアンスに接続するときに表示される [Login] ページ、セキュリティ アプライアンスのユーザ承認後に表示される [Home] ページ、ユーザがアプリケーションを起動するときに表示される [Application Access] ウィンドウ、およびユーザがクライアントレス SSL VPN セッションからログアウトするときに表示される [Logout] ページが含まれます。

ポータル ページのカスタマイズ後は、このカスタマイゼーションを保存して、特定の接続プロファイル、グループ ポリシー、またはユーザに適用できます。ASA をリロードするか、またはクライアントレス SSL をオフに切り替えてから再度イネーブルにするまで、変更は適用されません。

いくつものカスタマイゼーション オブジェクトを作成、保存して、個々のユーザまたはユーザグループに応じてポータル ページの外観を変更するようにセキュリティ アプライアンスをイネーブル化できます。

カスタマイゼーションに関する情報

ASA は、カスタマイゼーション オブジェクトを使用して、ユーザ画面の外観を定義します。カスタマイゼーション オブジェクトは、リモート ユーザに表示されるカスタマイズ可能なすべての画面項目に対する XML タグを含む XML ファイルからコンパイルされます。ASA ソフトウェアには、リモート PC にエクスポートできるカスタマイゼーション テンプレートが含まれています。このテンプレートを編集して、新しいカスタマイゼーション オブジェクトとして ASA にインポートし戻すことができます。

カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度 ASA にインポートできます。

カスタマイゼーション オブジェクト、接続プロファイル、およびグループ ポリシー

ユーザが初めて接続するときには、接続プロファイル（トンネル グループ）で指定されたデフォルトのカスタマイゼーション オブジェクト（*DfltCustomization*）がログイン画面の表示方法を決定します。接続プロファイル リストがイネーブルになっている場合に、独自のカスタマイゼーションがある別のグループをユーザが選択すると、その新しいグループのカスタマイゼーション オブジェクトを反映して画面が変わります。

リモート ユーザが認証された後は、画面の外観は、そのグループ ポリシーにカスタマイゼーション オブジェクトが割り当てられているかどうかによって決まります。

カスタマイゼーション テンプレートの編集

この項では、カスタマイゼーション テンプレートの内容を示して、便利な図を提供しています。これらを参照して、正しい XML タグをすばやく選択して、画面表示を変更できます。

テキスト エディタまたは XML エディタを使用して、XML ファイルを編集できます。次の例は、カスタマイゼーション テンプレートの XML タグを示しています。一部の冗長タグは、見やすくするために削除してあります。

例：

```
<custom>
   <localization>
      <languages>en,ja,zh,ru,ua</languages>
      <default-language>en</default-language>
   </localization>
    <auth-page>
      <window>
          <title-text l10n="yes"><![CDATA[SSL VPN Service]]></title-text>
      </window>
      <full-customization>
          <mode>disable</mode>
          <url></url>
      </full-customization>
      <language-selector>
        <mode>disable</mode>
```

```
          <title l10n="yes">Language:</title>
          <language>
            <code>en</code>
            <text>English</text>
          </language>
          <language>
            <code>zh</code>
            <text>ä¸-å›½ (Chinese)</text>
          </language>
          <language>
            <code>ja</code>
            <text>æ—¥æœ¬ (Japanese)</text>
          </language>
          <language>
            <code>ru</code>
            <text>Ð ÑƒÑÑкÐ¸Ð¹ (Russian)</text>
          </language>
          <language>
            <code>ua</code>
            <text>Ð£ÐºÑ?Ð°Ñ—Ð½ÑÑŒÐºÐ° (Ukrainian)</text>
          </language>
        </language-selector>
        <logon-form>
            <title-text l10n="yes"><![CDATA[Login]]></title-text>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <message-text l10n="yes"><![CDATA[Please enter your username and
password.]]></message-text>
            <username-prompt-text l10n="yes"><![CDATA[USERNAME:]]></username-prompt-text>
            <password-prompt-text l10n="yes"><![CDATA[PASSWORD:]]></password-prompt-text>
            <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
            <internal-password-first>no</internal-password-first>
            <group-prompt-text l10n="yes"><![CDATA[GROUP:]]></group-prompt-text>
            <submit-button-text l10n="yes"><![CDATA[Login]]></submit-button-text>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <font-color>#000000</font-color>
            <background-color>#ffffff</background-color>
            <border-color>#858A91</border-color>
        </logon-form>
        <logout-form>
            <title-text l10n="yes"><![CDATA[Logout]]></title-text>
            <message-text l10n="yes"><![CDATA[Goodbye.<br>

For your own security, please:<br>

<li>Clear the browser's cache

<li>Delete any downloaded files

<li>Close the browser's window]]></message-text>
            <login-button-text l10n="yes">Logon</login-button-text>
            <hide-login-button>no</hide-login-button>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <title-font-color><![CDATA[#ffffff]]></title-font-color>
            <title-background-color><![CDATA[#666666]]></title-background-color>
            <font-color>#000000</font-color>
            <background-color>#ffffff</background-color>
            <border-color>#858A91</border-color>
        </logout-form>
        <title-panel>
           <mode>enable</mode>
```

```
      <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
      <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
      <gradient>yes</gradient>
      <style></style>
      <background-color><![CDATA[#ffffff]]></background-color>
      <font-size><![CDATA[larger]]></font-size>
      <font-color><![CDATA[#800000]]></font-color>
      <font-weight><![CDATA[bold]]></font-weight>
  </title-panel>
  <info-panel>
    <mode>disable</mode>
    <image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
    <image-position>above</image-position>
    <text l10n="yes"></text>
  </info-panel>
  <copyright-panel>
     <mode>disable</mode>
     <text l10n="yes"></text>
  </copyright-panel>
</auth-page>
<portal>
  <title-panel>
     <mode>enable</mode>
     <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
     <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
     <gradient>yes</gradient>
     <style></style>
     <background-color><![CDATA[#ffffff]]></background-color>
     <font-size><![CDATA[larger]]></font-size>
     <font-color><![CDATA[#800000]]></font-color>
     <font-weight><![CDATA[bold]]></font-weight>
  </title-panel>
  <browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
  <access-network-title l10n="yes">Start AnyConnect</access-network-title>
  <application>
     <mode>enable</mode>
     <id>home</id>
     <tab-title l10n="yes">Home</tab-title>
     <order>1</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>web-access</id>
     <tab-title l10n="yes"><![CDATA[Web Applications]]></tab-title>
     <url-list-title l10n="yes"><![CDATA[Web Bookmarks]]></url-list-title>
     <order>2</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>file-access</id>
     <tab-title l10n="yes"><![CDATA[Browse Networks]]></tab-title>
     <url-list-title l10n="yes"><![CDATA[File Folder Bookmarks]]></url-list-title>
     <order>3</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>app-access</id>
     <tab-title l10n="yes"><![CDATA[Application Access]]></tab-title>
     <order>4</order>
  </application>
  <application>
     <mode>enable</mode>
     <id>net-access</id>
     <tab-title l10n="yes">AnyConnect</tab-title>
```

```
            <order>4</order>
         </application>
         <application>
            <mode>enable</mode>
            <id>help</id>
            <tab-title l10n="yes">Help</tab-title>
            <order>1000000</order>
         </application>
         <toolbar>
            <mode>enable</mode>
            <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
            <prompt-box-title l10n="yes">Address</prompt-box-title>
            <browse-button-text l10n="yes">Browse</browse-button-text>
         </toolbar>
         <column>
            <width>100%</width>
            <order>1</order>
         </column>
         <pane>
            <type>TEXT</type>
            <mode>disable</mode>
            <title></title>
            <text></text>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>IMAGE</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>HTML</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>RSS</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <url-lists>
            <mode>group</mode>
         </url-lists>
         <home-page>
            <mode>standard</mode>
            <url></url>
         </home-page>
      </portal>
   </custom>
```

図 17-4 に、[Login] ページとページをカスタマイズする XML タグを示します。これらのタグはすべて、上位レベルのタグ <auth-page> にネストされています。

図 17-4　[Login] ページと関連の XML タグ

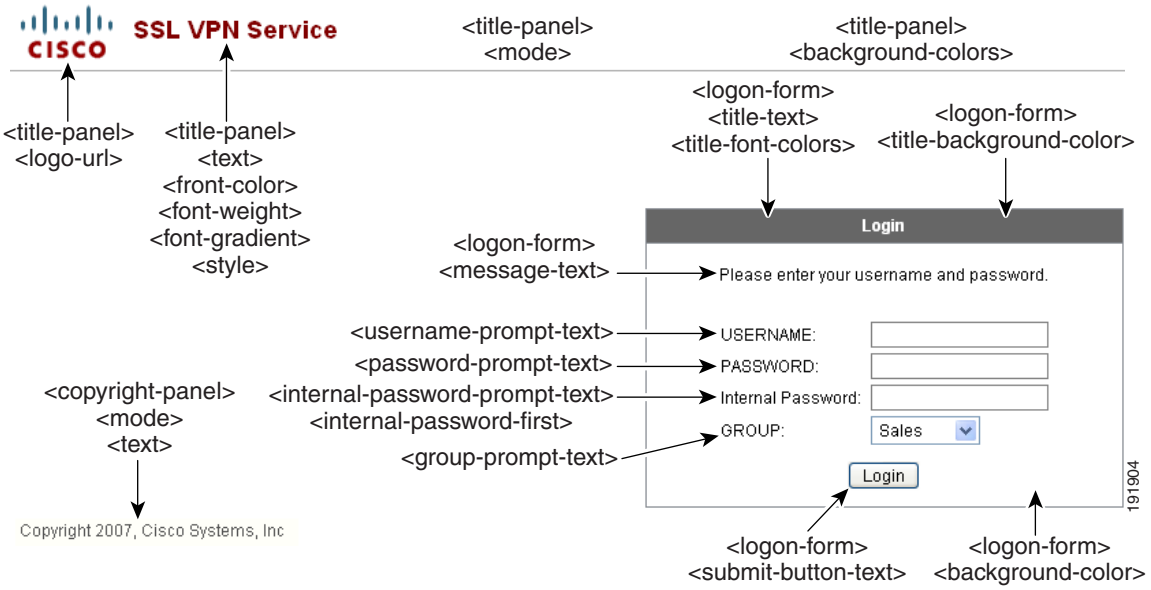


図 17-5 は、[Login] ページで使用可能な言語セレクタ ドロップダウン リストと、この機能をカスタマイズするための XML タグを示しています。これらのタグはすべて、上位レベルの <auth-page> タグにネストされています。

図 17-5　[Login] 画面上の言語セレクタと関連の XML タグ

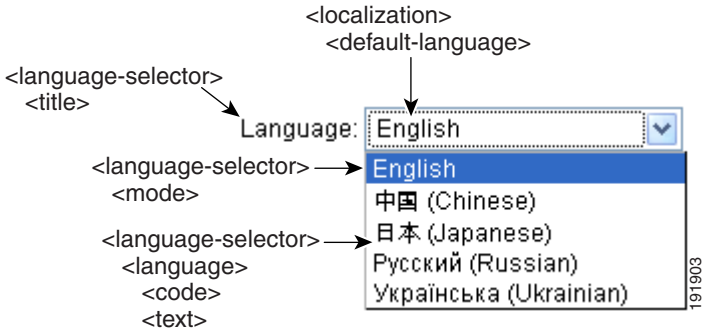


図 17-6 は、[Login] ページで使用できる Information Panel とこの機能をカスタマイズするための XML タグを示しています。この情報は [Login] ボックスの左側または右側に表示されます。これらのタグは、上位レベルの <auth-page> タグにネストされています。

図 17-6　[Login] 画面上の Information Panel と関連の XML タグ

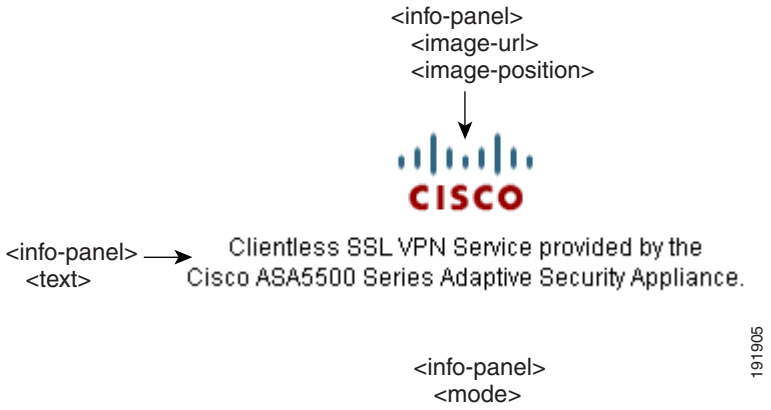
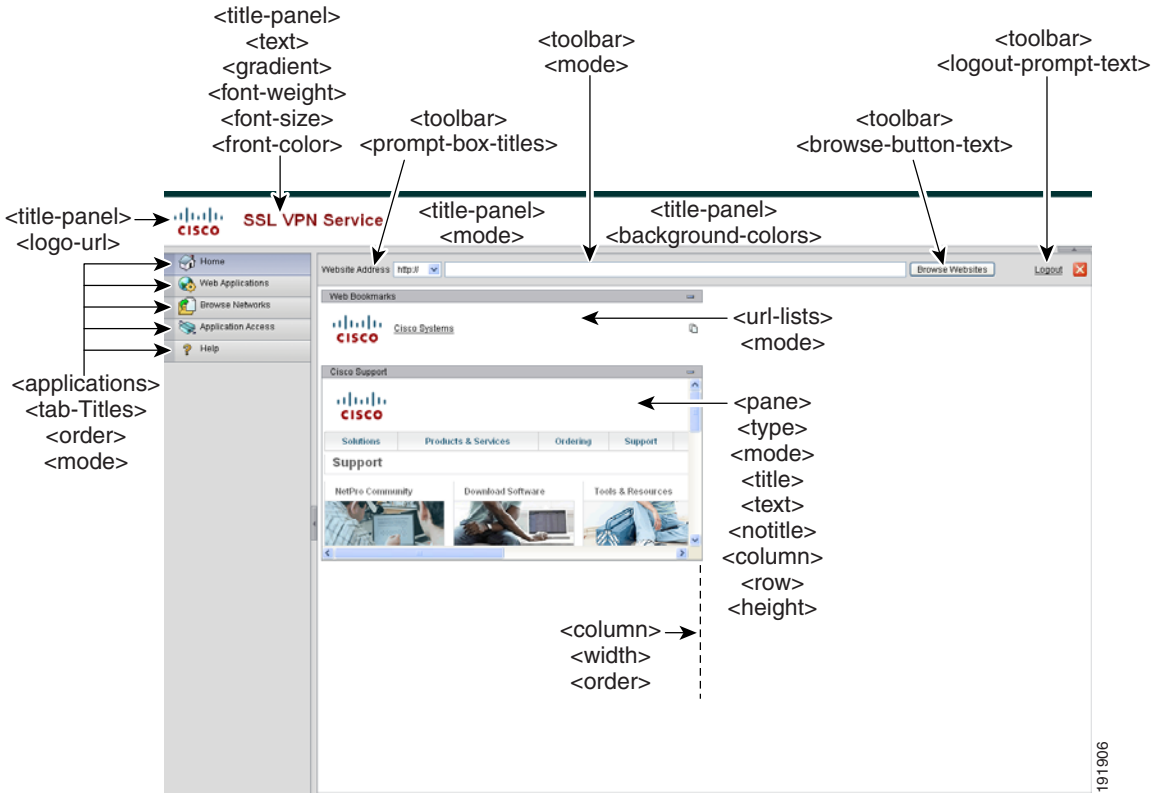


図 17-7 は、ポータル ページとこの機能をカスタマイズするための XML タグを示しています。これらのタグは、上位レベルの <auth-page> タグにネストされています。

図 17-7　ポータル ページと関連の XML タグ



ログイン画面の高度なカスタマイゼーション

提供されるログイン画面の特定の画面要素を変更するのではなく、独自のカスタム ログイン画面を使用する場合は、*フル カスタマイゼーション*機能を使用してこの高度なカスタマイゼーションを実行できます。

フル カスタマイゼーションを使用して、独自のログイン画面の HTML を入力し、ASA で関数を呼び出す Cisco HTML コードを挿入します。これで、Login フォームと言語セレクタ ドロップダウン リストが作成されます。

この項では、独自の HTML コードを作成するために必要な修正内容、および ASA が独自のコードを使用する場合に設定する必要があるタスクについて説明します。

図 17-8 に、クライアントレス SSL VPN ユーザに表示される標準の Cisco ログイン画面を示します。Login フォームは、HTML コードで呼び出す関数によって表示されます。

図 17-8　　標準の Cisco [Login] ページ

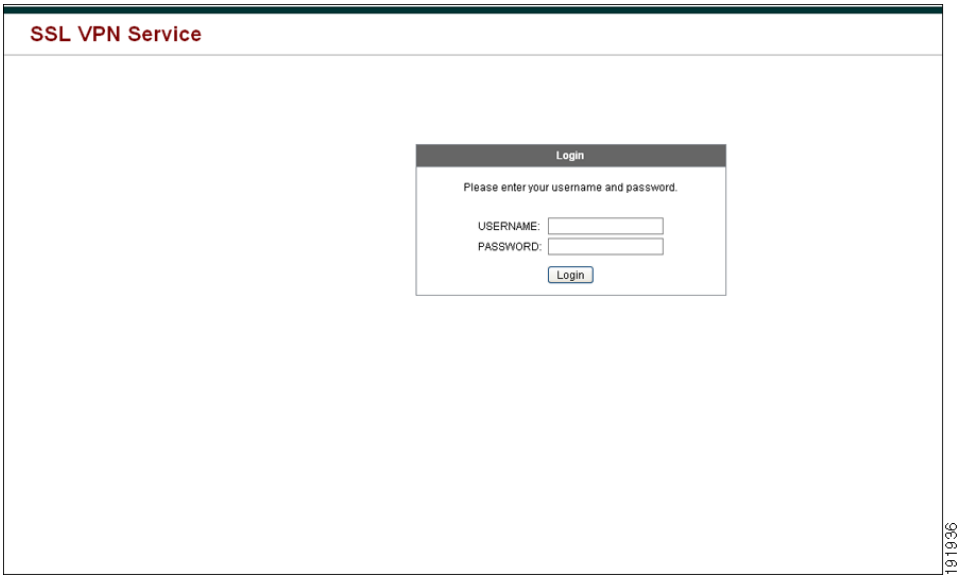
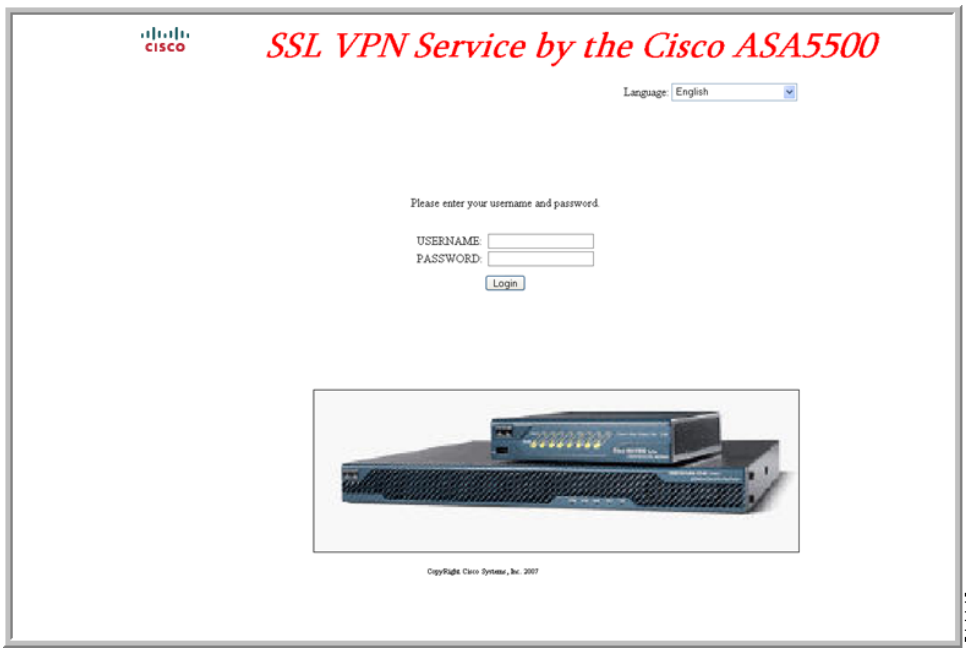


図 17-9 に、言語セレクタ ドロップダウン リストを示します。この機能は、クライアントレス SSL VPN ユーザにはオプションとなっており、ログイン画面の HTML コード内の関数によっても呼び出されます。

図 17-9　　言語セレクタ ドロップダウン リスト

図 17-10 は、フル カスタマイゼーション機能によってイネーブル化される簡単なカスタム ログイン画面の例を示しています。

図 17-10　　ログイン画面のフル カスタマイゼーション例



次の HTML コードは例として使用され、表示するコードです。

例：

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font
color="#FF0000" size="7" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font></b></i></p>

    <body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

    <table>

    <tr><td colspan=3 height=20 align=right><div id="selector" style="width:
    300px"></div></td></tr>
    <tr><td></td><td></td><td></td></tr>
    <tr>
    <td height="379"></td>
    <td height="379"></td>
    <td align=middle valign=middle>
    <div id=lform >
    <p> </p>
    <p> </p>
```

```
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

字下げされたコードは、画面に Login フォームと言語セレクタを挿入します。関数 **csco_ShowLoginForm('lform')** は Login フォームを挿入します。**csco_ShowLanguageSelector('selector')** は、言語セレクタを挿入します。

HTML ファイルの変更

ステップ 1　ファイルに **login.inc** という名前を付けます。このファイルをインポートすると、ASA はこのファイル名をログイン画面として認識します。

ステップ 2　このファイルで使用されるイメージのパスに **/+CSCOU+/** を含めるように変更します。

認証前にリモート ユーザに表示されるファイルは、パス /+CSCOU+/ で表される ASA のキャッシュ メモリの特定のエリアに置く必要があります。そのため、このファイルにある各イメージのソースはこのパスに含める必要があります。次に例を示します。

```
src="/+CSCOU+/asa5520.gif"
```

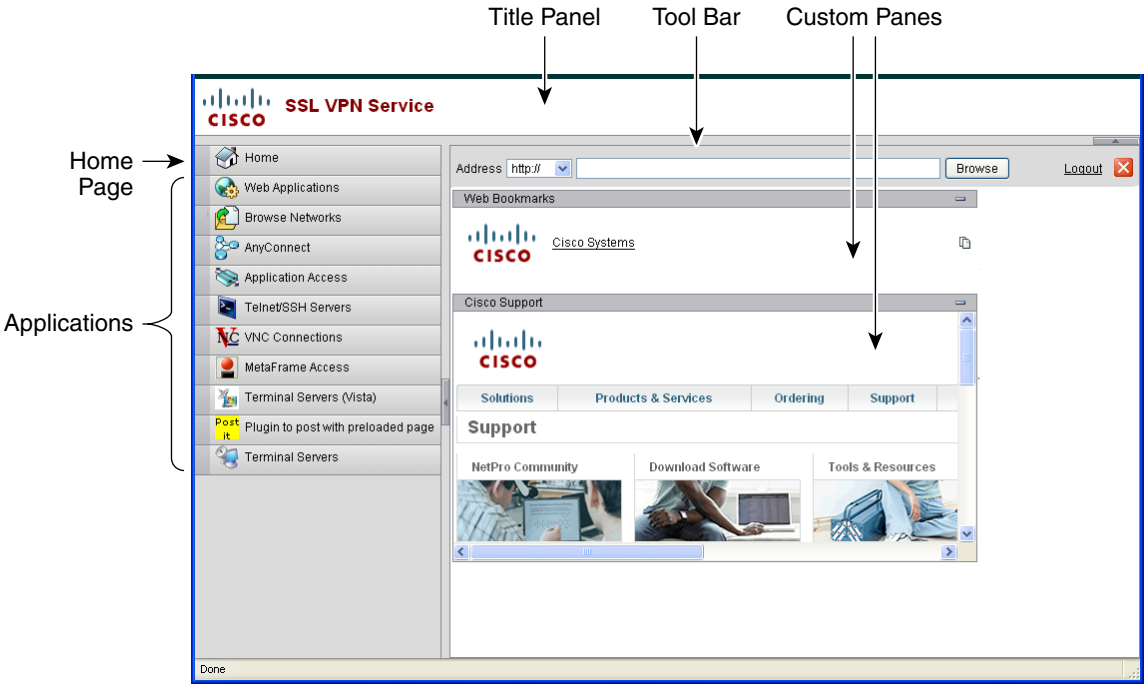
ステップ 3　下記の特別な HTML コードを挿入します。このコードには、Login フォームと言語セレクタを画面に挿入する前述のシスコの関数が含まれています。

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

ポータル ページのカスタマイズ

図 17-11 に、ポータル ページとカスタマイズ可能な事前定義されたコンポーネントを示します。

図 17-11　ポータル ページのカスタマイズ可能なコンポーネント



ページのコンポーネントをカスタマイズする以外に、ポータル ページを、テキスト、イメージ、RSS フィード、または HTML を表示するカスタム ペインに分割できます。

ポータル ページをカスタマイズするには、次の手順を実行します。[Preview] ボタンをクリックして、各コンポーネントに対する変更をプレビューできます。

ステップ 1　[Portal Page] に移動し、ブラウザ ウィンドウのタイトルを指定します。

ステップ 2　タイトル パネルを表示し、カスタマイズします。[Portal Page] > [Title Panel] の順に選択し、[Display title panel] をオンにします。タイトルとして表示するテキストを入力し、ロゴを指定します。フォント スタイルを指定します。

ステップ 3　ツールバーをイネーブルにしてカスタマイズします。[Portal Page] > [Toolbar] の順に選択し、[Display toolbar] をオンにします。プロンプト ボックス、参照ボタン、およびログアウト プロンプトを必要に応じてカスタマイズします。

ステップ 4　アプリケーション リストをカスタマイズします。[Portal Page] > [Applications] の順に選択し、[Show navigation panel] をオンにします。テーブルに入力されているアプリケーションは ASA の設定でイネーブルにしたアプリケーションであり、クライアント/サーバ プラグインやポート転送アプリケーションが含まれています。

ステップ 5　ポータル ページ スペースでカスタム ペインを作成します。[Portal Page] > [Custom Panes] の順に選択し、必要に応じて、ウィンドウをテキスト、イメージ、RSS フィード、または HTML ページの行およびカラムに分割します。

ステップ 6　ホームページの URL を指定します。[Portal Page] > [Home Page] の順に選択し、[Enable custom intranet Web page] をオンにします。ブックマークの構成を定義するブックマーク モードを選択します。

タイムアウト アラート メッセージおよびツールチップを設定します。[Portal Page] > [Timeout Alerts] の順に選択します。

次の作業

カスタム ポータル タイムアウト アラートの設定について確認してください。

カスタム ポータル タイムアウト アラートの設定

クライアントレス SSL VPN 機能のユーザが VPN セッションで時間を管理できるように、クライアントレス SSL VPN ポータル ページには、クライアントレス VPN セッションが終了するまでの合計残り時間を示すカウントダウン タイマーが表示されます。セッションは、非アクティブ状態によって、または設定された最大許容接続時間が終了したために、タイムアウトします。

ユーザのセッションが、アイドル タイムアウトまたはセッション タイムアウトにより終了することをユーザに警告するカスタム メッセージを作成できます。デフォルトのアイドル タイムアウト メッセージはカスタム メッセージによって置き換えられます。デフォルトのメッセージは、「`Your session will expire in %s .`」です。メッセージ内の **%s** プレース ホルダは、進行するカウントダウン タイマーで置き換えられます。

ステップ 1　ASDM を起動し、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Customization] を選択します。

ステップ 2　[Add] をクリックして新しいカスタマイゼーション オブジェクトを追加するか、既存のカスタマイゼーション オブジェクトを選択して [Edit] をクリックし、カスタム アイドル タイムアウト メッセージを既存のカスタマイゼーション オブジェクトに追加します。

ステップ 3　[Add / Edit Customization Object] ペインで、ナビゲーション ツリーの [Portal Page] ノードを展開して、[Timeout Alerts] をクリックします。

ステップ 4　[Enable alert visual tooltip (red background for timer countdown)] をオンにします。これにより、カウントダウン タイマーがツール ヒントとして赤の背景に表示されます。ユーザが [Time left] 領域をクリックすると、時間領域が拡大されて、カスタム タイムアウト アラート メッセージが表示されます。このボックスをオフのままにしておくと、カスタム タイムアウト アラートはポップアップ ウィンドウに表示されます。

ステップ 5　[Idle Timeout Message] ボックスおよび [Session Timeout Message] ボックスにメッセージを入力します。メッセージの例は、次のとおりです。「`Warning: Your session will end in %s.Please complete your work and prepare to close your applications.`」

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。

カスタマイゼーション オブジェクト ファイルでのカスタム タイムアウト アラートの指定

必要に応じて、ASA の外部の既存のカスタマイゼーション オブジェクト ファイルを編集し、ASA にインポートできます。

タイムアウト メッセージは、XML カスタマイゼーション オブジェクト ファイルの <timeout-alerts> XML 要素で設定されます。<timeout-alerts> 要素は <portal> 要素の子です。<portal> 要素は <custom> 要素の子です。

<timeout-alerts> 要素は、<portal> の子要素の順序では、<home-page> 要素の後、<application> 要素の前に配置します。

<timeout-alerts> の次の子要素を指定する必要があります。

- <alert-tooltip> :「yes」に設定されると、カウントダウン タイマーはユーザにツール ヒントとして赤の背景に表示されます。カウントダウン タイマーをクリックすると、ツールチップが展開されて、カスタム メッセージが表示されます。「no」に設定されるか未定義の場合、カスタム メッセージはポップアップ ウィンドウでユーザに表示されます。
- <session-timeout-message> : この要素にカスタム セッション タイムアウト メッセージを入力します。設定されており、空ではない場合は、デフォルト メッセージの代わりに、カスタム メッセージを受け取ります。メッセージ内の %s プレース ホルダは、進行するカウントダウン タイマーで置き換えられます。
- <idle-timeout-message> : この要素にカスタム アイドル タイムアウト メッセージを入力します。設定されており、空ではない場合は、デフォルト メッセージの代わりに、カスタム メッセージを受け取ります。%s プレース ホルダは、進行するカウントダウン タイマーで置き換えられます。

次の作業

カスタマイゼーション オブジェクトのインポートおよびエクスポートと、XML ベースのポータル カスタマイゼーション オブジェクトと URL リストの作成について確認してください。

タイムアウト アラート要素および子要素の設定例

この例では、<portal> 要素の <timeout-alerts> 要素のみを示します。

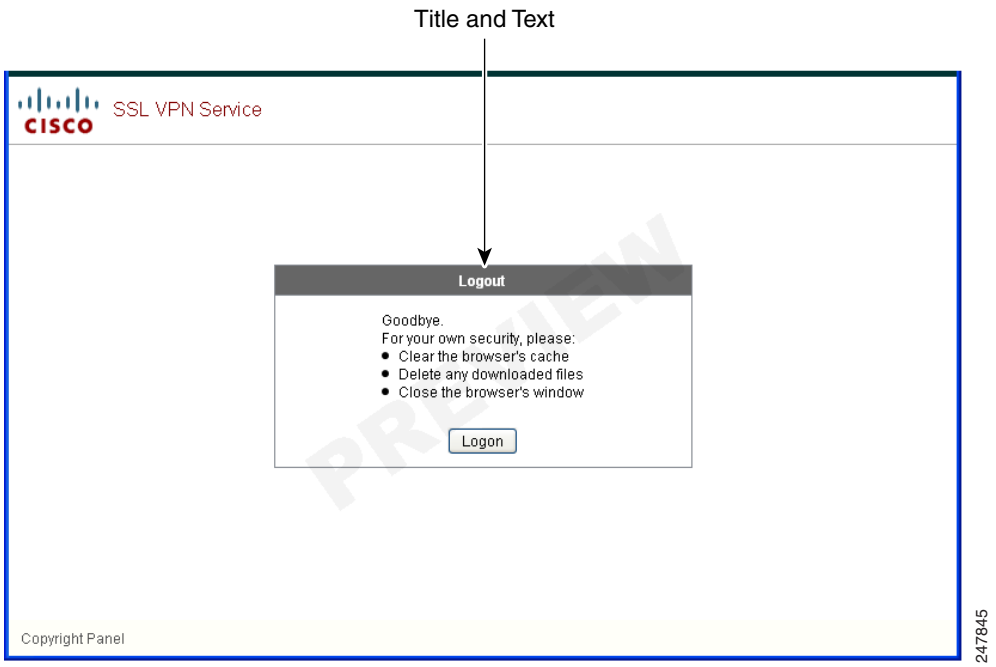
（注） この例を既存のカスタマイゼーション オブジェクトにカット アンド ペーストしないでください。

```
<portal>
    <window></window>
    <title-panel></title-panel>
    <toolbar></toolbar>
    <url-lists></url-lists>
    <navigation-panel></navigation-panel>
    <home-page>
    <timeout-alerts>
        <alert-tooltip>yes</alert-tooltip>
        <idle-timeout-message>You session expires in %s due to idleness.</idle-timeout-message>
        <session-timeout-message>Your session expires in %s.</session-timeout-message>
    </timeout-alerts>
    <application></application>
    <column></column>
    <pane></pane>
    <external-portal></external-portal>
</portal>
```

ログアウト ページのカスタマイズ

図 17-12 に、カスタマイズ可能なログアウト ページを示します。

図 17-12　ログアウト ページのコンポーネント



ログアウト ページをカスタマイズするには、次の手順を実行します。[Preview] ボタンをクリックして、各コンポーネントに対する変更をプレビューできます。

ステップ 1　[Logout Page] に移動します。必要に応じて、タイトルまたはテキストをカスタマイズします。

ステップ 2　ユーザに便利なように、ログアウト ページに [Login] ボタンを表示できます。そのためには、[Show logon button] をオンにします。必要に応じて、ボタンのテキストをカスタマイズします。

ステップ 3　必要に応じて、タイトルのフォントまたは背景をカスタマイズします。

ステップ 4　[OK] をクリックしてから、編集したカスタマイゼーション オブジェクトに変更を適用します。

カスタマイゼーション オブジェクトの追加

ステップ 1　[Add] をクリックし、新しいカスタマイゼーション オブジェクトの名前を入力します。最大 64 文字で、スペースは使用できません。

ステップ 2　（オプション）[Find] をクリックして、カスタマイゼーション オブジェクトを検索します。このフィールドへの入力を開始すると、各フィールドの先頭部分の文字が検索され、一致するものが検出されます。ワイルドカードを使用すると、検索範囲が広がります。たとえば、[Find] フィールドに *sal* と入力すると、sales という名前のカスタマイゼーション オブジェクトは一致しますが、wholesalers という名前のカスタマイゼーション オブジェクトは一致しません。[Find] フィールドに **sal* と入力した場合は、テーブル内の sales と wholesalers のうち、最初に出現するものが検出されます。

上矢印と下矢印を使用して、上または下にある、一致する次の文字列に移動します。[Match Case] チェックボックスをオンにして、大文字と小文字が区別されるようにします。

ステップ 3　オンスクリーン キーボードをポータル ページ上にいつ表示するかを指定します。次の選択肢があります。

- Do not show OnScreen Keyboard
- Show only for the login page
- Show for all portal pages requiring authentication

ステップ 4　（オプション）カスタマイゼーション オブジェクトを強調表示し、[Assign] をクリックして、選択したオブジェクトを 1 つ以上のグループ ポリシー、接続プロファイル、または LOCAL ユーザに割り当てます。

カスタマイゼーション オブジェクトのインポートおよびエクスポート

既存のカスタマイゼーション オブジェクトをインポートまたはエクスポートできます。エンドユーザに適用するオブジェクトをインポートします。ASA にすでに存在するカスタマイゼーション オブジェクトは、編集のためにエクスポートし、その後再インポートできます。

ステップ 1　カスタマイゼーション オブジェクトを名前で指定します。最大 64 文字で、スペースは使用できません。

ステップ 2　カスタマイゼーション ファイルをインポートする、またはエクスポートするための方法を選択します。

- [Local computer]：ローカル PC にあるファイルをインポートする場合は、この方式を選択します。
- [Path]：ファイルへのパスを入力します。
- [Browse Local Files]：ファイルへのパスを参照します。
- [Flash file system]：ASA に常駐するファイルをエクスポートするには、この方式を選択します。
- [Path]：ファイルへのパスを入力します。
- [Browse Flash]：ファイルへのパスを参照します。
- [Remote server]：ASA からアクセスできるリモート サーバに常駐するカスタマイゼーション ファイルをインポートするには、このオプションを選択します。
- [Path]：ファイルにアクセスする方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。

ステップ 3　クリックして、ファイルをインポートまたはエクスポートします。

XML カスタマイゼーション ファイルの構成について

表 17-1 に、XML カスタマイゼーション オブジェクトのファイル構造を示します。

（注）　パラメータ/タグが指定されなければデフォルト/継承値が使用されます。存在する場合は、空の文字列であってもパラメータ/タグ値が設定されます。

表 17-1　XML ベース カスタマイゼーション ファイルの構造

タグ	タイプ	値	プリセット値	説明
custom	**ノード**	—	—	**ルート タグ**
auth-page	**ノード**	—	—	**認証ページ コンフィギュレーションのタグ コンテナ**
window	**ノード**	—	—	**ブラウザ ウィンドウ**
title-text	ストリング	任意の文字列	空の文字列	—
title-panel	**ノード**	—	—	**ロゴおよびテキストを表示したページの先頭パネル**
mode	テキスト	enable|disable	disable	—
text	テキスト	任意の文字列	空の文字列	—
logo-url	テキスト	任意の URL	空のイメージ URL	—
copyright-panel	**ノード**	—	—	**著作権情報を示したページの下部ペイン**
mode	テキスト	enable|disable	disable	—
text	テキスト	任意の URL	空の文字列	—
info-panel	**ノード**	—	—	**カスタム テキストとイメージを表示したペイン**
mode	ストリング	enable|disable	disable	—
image-position	ストリング	above|below	above	テキストに対する相対的なイメージの位置
image-url	ストリング	任意の URL	空のイメージ	—
text	ストリング	任意の文字列	空の文字列	—
logon-form	**ノード**	—	—	**ユーザ名、パスワード、グループ プロンプトのフォーム**
title-text	ストリング	任意の文字列	Logon	—
message-text	ストリング	任意の文字列	空の文字列	—
username-prompt-text	ストリング	任意の文字列	Username	—

表 17-1　XML ベース カスタマイゼーション ファイルの構造 （続き）

password-prompt-text	ストリング	任意の文字列	Password	—
internal-password-prompt-text	ストリング	任意の文字列	Internal Password	—
group-prompt-text	ストリング	任意の文字列	Group	—
submit-button-text	ストリング	任意の文字列	Logon	
logout-form	**ノード**	—	—	**ログアウト メッセージと、ログインまたはウィンドウを閉じるためのボタンを表示したフォーム**
title-text	ストリング	任意の文字列	Logout	—
message-text	ストリング	任意の文字列	空の文字列	—
login-button-text	ストリング	任意の文字列	Login	
close-button-text	ストリング	任意の文字列	Close window	—
language-selector	**ノード**	—	—	**言語を選択するドロップダウン リスト**
mode	ストリング	enableldisable	disable	—
title	テキスト	—	Language	言語を選択するよう求めるプロンプト テキスト
language	**ノード（複数）**	—	—	—
code	ストリング	—	—	—
text	ストリング	—	—	—
portal	**ノード**	—	—	**ポータル ページ コンフィギュレーションのタグコンテナ**
window	**ノード**	—	—	**認証ページの説明を参照**
title-text	ストリング	任意の文字列	空の文字列	—
title-panel	**ノード**	—	—	**認証ページの説明を参照**
mode	ストリング	enableldisable	Disable	—
text	ストリング	任意の文字列	空の文字列	—
logo-url	ストリング	任意の URL	空のイメージ URL	—
navigation-panel	**ノード**	—	—	**アプリケーション タブの左側のペイン**
mode	ストリング	enableldisable	enable	—

表 17-1　XML ベース カスタマイゼーション ファイルの構造 （続き）

application	**ノード（複数）**	—	**該当なし**	**ノードは（ID によって）設定されているアプリケーションのデフォルトを変更する**
id	ストリング	ストック アプリケーションの場合： web-access file-access app-access net-access help ins の場合： 固有のプラグイン	該当なし	—
tab-title	ストリング	—	該当なし	—
order	数値	—	該当なし	エレメントの並べ替えで使用する値。デフォルトのエレメント順の値には、1000、2000、3000 などの段階があります。たとえば、最初と 2 番目のエレメントの間にエレメントを挿入するには、1001 ～ 1999 の値を使用します。
url-list-title	ストリング	—	該当なし	アプリケーションにブックマークがある場合は、グループ化されたブックマークを表示したパネルのタイトル
mode	ストリング	enable|disable	該当なし	v
toolbar	**ノード**	—	—	—
mode	ストリング	enable|disable	Enable	—
prompt-box-title	ストリング	任意の文字列	Address	URL プロンプト リストのタイトル
browse-button-text	ストリング	任意の文字列	Browse	[Browse] ボタンのテキスト
logout-prompt-text	ストリング	任意の文字列	Logout	—
column	**ノード（複数）**	—	—	**デフォルトで 1 列を表示**
width	ストリング	—	該当なし	—

表 17-1　XML ベース カスタマイゼーション ファイルの構造 （続き）

order	数値	—	該当なし	エレメントの並べ替えで使用する値。
url-lists	**ノード**	—	—	**URL リストは、明示的にオフに切り替えられていない場合、ポータル ホーム ページのデフォルト エレメントと見なされる**
mode	ストリング	group | nogroup	group	モード： group：Web Bookmarks や File Bookmarks などのアプリケーション タイプによってグループ化されたエレメント no-group：URL リストを別々のペインに表示する disable：デフォルトで URL リストを表示しない
panel	ノード （複数）	—	—	追加ペインの設定を許可
mode	ストリング	enable|disable	—	コンフィギュレーションを削除せずにパネルを一時的にオフに切り替える場合に使用する
title	ストリング	—	—	—
type	ストリング	—	—	サポートされるタイプ： RSS IMAGE TEXT HTML
url	ストリング	—	—	RSS、IMAGE、または HTML タイプのペインの URL
url-mode	ストリング	—	—	モード：mangle、no-mangle
text	ストリング	—	—	TEXT タイプ ペインのテキスト
column	数値	—	—	—

カスタマイゼーションの設定例

次の例は、次のカスタマイゼーション オプションを示しています。

- File アクセス アプリケーションのタブを非表示にする。
- Web Access アプリケーションのタイトルと順序を変更する。
- ホーム ページで 2 つのカラムを定義する。
- RSS ペインを追加する。
- 2 番目のペインの上部に 3 つのペイン（テキスト、イメージ、および html）を追加する。

```
<custom name="Default">
  <auth-page>

    <window>
          <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
         <mode>enable</mode>
         <text l10n="yes">EXAMPLE WebVPN</text>
         <logo-url>http://www.example.com/images/EXAMPLE.gif</logo-url>
    </title-panel>

    <copyright>
         <mode>enable</mode>
         <text l10n="yes">(c)Copyright, EXAMPLE Inc., 2006</text>
    </copyright>

    <info-panel>
        <mode>enable</mode>
        <image-url>/+CSCOE+/custom/EXAMPLE.jpg</image-url>
      <text l10n="yes">
            <![CDATA[
            <div>
            <b>Welcome to WebVPN !.</b>
            </div>
            ]]>
      </text>
    </info-panel>
    <logon-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <username-prompt-text l10n="yes">Username</username-prompt-text>
          <password-prompt-text l10n="yes">Password</password-prompt-text>
          <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
          <group-prompt-text l10n="yes">Group</group-prompt-text>
          <submit-button-text l10n="yes">Logon</submit-button-text>
      </form>
    </logon-form>
    <logout-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <login-button-text l10n="yes">Login</login-button-text>
          <close-button-text l10n="yes">Logon</close-button-text>
      </form>
    </logout-form>
```

```
  <language-slector>
    <language>
        <code l10n="yes">code1</code>
        <text l10n="yes">text1</text>
    </language>
    <language>
        <code l10n="yes">code2</code>
        <text l10n="yes">text2</text>
    </language>
  </language-slector>

</auth-page>
<portal>

  <window>
        <title-text l10n="yes">title WebVPN Logon</title>
  </window>

  <title-panel>
       <mode>enable</mode>
       <text l10n="yes">EXAMPLE WebVPN</text>
       <logo-url>http://www.example.com/logo.gif</logo-url>
  </title-panel>

  <navigation-panel>
       <mode>enable</mode>
  </navigation-panel>

  <application>
          <id>file-access</id>
          <mode>disable</mode>
  </application>
  <application>
          <id>web-access</id>
          <tab-title>EXAMPLE Intranet</tab-title>
          <order>3001</order>
  </application>

 <column>
          <order>2</order>
          <width>40%</width>
<column>
 <column>
          <order>1</order>
          <width>60%</width>
<column>

<url-lists>
  <mode>no-group</mode>
</url-lists>

<pane>
 <id>rss_pane</id>
  <type>RSS</type>
 <url>rss.example.com?id=78</url>
</pane>
<pane>
  <type>IMAGE</type>
 <url>http://www.example.com/logo.gif</url>
  <column>1</column>
  <row>2</row>
 </pane>

<pane>
```

```
    <type>HTML</type>
   <title>EXAMPLE news</title>
   <url>http://www.example.com/news.html</url>
    <column>1</column>
    <row>3</row>
   </pane>

  </portal>

</custom>
```

カスタマイゼーション テンプレートの使用

Template という名前のカスタマイゼーション テンプレートには、現在使用されているタグすべてと、その使用法を説明した対応するコメントが含まれています。**export** コマンドを使用し、次のようにして ASA からカスタマイゼーション テンプレートをダウンロードします。

```
hostname# export webvpn customization Template tftp://webserver/default.xml
hostname#
```

Template ファイルは、変更または削除できません。この例のようにしてエクスポートする場合は、*default.xml* という新しい名前で保存します。このファイルで変更を行った後、組織の必要を満たすカスタマイゼーション オブジェクトを作成し、*default.xml* または選択する別の名前のファイルとして ASA にインポートします。次に例を示します。

```
hostname# import webvpn customization General tftp://webserver/custom.xml
hostname#
```

ここで *custom.xml* という名前の XML オブジェクトをインポートし、ASA で *General* と命名します。

カスタマイゼーション テンプレート

Template という名前のカスタマイゼーション テンプレートを次に示します。

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--

Copyright (c) 2008,2009 by Cisco Systems, Inc.
All rights reserved.

Note: all white spaces in tag values are significant and preserved.


Tag: custom
Description: Root customization tag

Tag: custom/languages
Description: Contains list of languages, recognized by ASA
Value: string containing comma-separated language codes.Each language code is
       a set dash-separated alphanumeric characters, started with
       alpha-character (for example: en, en-us, irokese8-language-us)
Default value: en-us
Tag: custom/default-language
Description: Language code that is selected when the client and the server
             were not able to negotiate the language automatically.
             For example the set of languages configured in the browser
```

```
            is "en,ja", and the list of languages, specified by
            'custom/languages' tag is "cn,fr", the default-language will be
            used.
Value: string, containing one of the language coded, specified in
'custom/languages' tag above.
Default value: en-us

*********************************************************

Tag: custom/auth-page
Description: Contains authentication page settings

*********************************************************
Tag: custom/auth-page/window
Description: Contains settings of the authentication page browser window

Tag: custom/auth-page/window/title-text
Description: The title of the browser window of the authentication page
Value: arbitrary string
Default value: Browser's default value

*********************************************************

Tag: custom/auth-page/title-panel
Description: Contains settings for the title panel

Tag: custom/auth-page/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable
Tag: custom/auth-page/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-page/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder,lighter etc.
Default value: empty string

Tag: custom/auth-page/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string



Tag: custom/auth-page/title-panel/gradient
```

```
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/auth-page/title-panel/style
Description: CSS style of the title panel
Value: CSS style string
Default value: empty string

*******************************************************

Tag: custom/auth-page/copyright-panel
Description: Contains the copyright panel settings

Tag: custom/auth-page/copyright-panel/mode
Description: The copyright panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/copyright-panel/text
Description: The copyright panel text
Value: arbitrary string
Default value: empty string

*******************************************************
Tag: custom/auth-page/info-panel
Description: Contains information panel settings

Tag: custom/auth-page/info-panel/mode
Description: The information panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/info-panel/image-position
Description: Position of the image, above or below the informational panel text
Values: above|below
Default value: above

Tag: custom/auth-page/info-panel/image-url
Description: URL of the information panel image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/info-panel/text
Description: Text of the information panel
Text: arbitrary string
Default value: empty string

*******************************************************

Tag: custom/auth-page/logon-form
Description: Contains logon form settings

Tag: custom/auth-page/logon-form/title-text
Description: The logon form title text
Value: arbitrary string
Default value: "Logon"

Tag: custom/auth-page/logon-form/message-text
Description: The message inside of the logon form
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/logon-form/username-prompt-text
Description: The username prompt text
```

```
Value: arbitrary string
Default value: "Username"

Tag: custom/auth-page/logon-form/password-prompt-text
Description: The password prompt text
Value: arbitrary string
Default value: "Password"

Tag: custom/auth-page/logon-form/internal-password-prompt-text
Description: The internal password prompt text
Value: arbitrary string
Default value: "Internal Password"

Tag: custom/auth-page/logon-form/group-prompt-text
Description: The group selector prompt text
Value: arbitrary string
Default value: "Group"


Tag: custom/auth-page/logon-form/submit-button-text
Description: The submit button text
Value: arbitrary string
Default value: "Logon"

Tag: custom/auth-page/logon-form/internal-password-first
Description: Sets internal password first in the order
Value: yes|no
Default value: no


Tag: custom/auth-page/logon-form/title-font-color
Description: The font color of the logon form title
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/logon-form/title-background-color
Description: The background color of the logon form title
Value: HTML color format, for example #FFFFFF
Default value: #000000


Tag: custom/auth-page/logon-form/font-color
Description: The font color of the logon form
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/logon-form/background-color
Description: The background color of the logon form
Value: HTML color format, for example #FFFFFF
Default value: #000000


*******************************************************

Tag: custom/auth-page/logout-form
Description: Contains the logout form settings

Tag: custom/auth-page/logout-form/title-text
Description: The logout form title text
Value: arbitrary string
Default value: "Logout"

Tag: custom/auth-page/logout-form/message-text
Description: The logout form message text
Value: arbitrary string
```

```
Default value: Goodbye.
               For your own security, please:
               Clear the browser's cache
               Delete any downloaded files
               Close the browser's window

Tag: custom/auth-page/logout-form/login-button-text
Description: The text of the button sending the user to the logon page
Value: arbitrary string
Default value: "Logon"

*********************************************************

Tag: custom/auth-page/language-selector
Description: Contains the language selector settings

Tag: custom/auth-page/language-selector/mode
Description: The language selector mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/language-selector/title
Description: The language selector title
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/language-selector/language (multiple)
Description: Contains the language settings

Tag: custom/auth-page/language-selector/language/code
Description: The code of the language
Value (required): The language code string

Tag: custom/auth-page/language-selector/language/text
Description: The text of the language in the language selector drop-down box
Value (required): arbitrary string

*********************************************************

Tag: custom/portal
Description: Contains portal page settings

*********************************************************

Tag: custom/portal/window
Description: Contains the portal page browser window settings

Tag: custom/portal/window/title-text
Description: The title of the browser window of the portal page
Value: arbitrary string
Default value: Browser's default value

*********************************************************

Tag: custom/portal/title-panel
Description: Contains settings for the title panel

Tag: custom/portal/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable

Tag: custom/portal/title-panel/text
Description: The title panel text.
Value: arbitrary string
```

```
Default value: empty string

Tag: custom/portal/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/portal/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-pa/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/portal/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder,lighter etc.
Default value: empty string

Tag: custom/portal/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string
Tag: custom/portal/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/portal/title-panel/style
Description: CSS style for title text
Value: CSS style string
Default value: empty string

*******************************************************

Tag: custom/portal/application (multiple)
Description: Contains the application setting

Tag: custom/portal/application/mode
Description: The application mode
Value: enable|disable
Default value: enable

Tag: custom/portal/application/id
Description: The application ID.Standard application ID's are: home, web-access,
file-access, app-access, network-access, help
Value: The application ID string
Default value: empty string

Tag: custom/portal/application/tab-title
Description: The application tab text in the navigation panel
Value: arbitrary string
Default value: empty string

Tag: custom/portal/application/order
Description: The order of the application's tab in the navigation panel.Applications with
lesser order go first.
Value: arbitrary number
Default value: 1000

Tag: custom/portal/application/url-list-title
```

```
Description: The title of the application's URL list pane (in group mode)
Value: arbitrary string
Default value: Tab tite value concatenated with "Bookmarks"

*******************************************************

Tag: custom/portal/navigation-panel
Description: Contains the navigation panel settings

Tag: custom/portal/navigation-panel/mode
Description: The navigation panel mode
Value: enable|disable
Default value: enable

*******************************************************

Tag: custom/portal/toolbar
Description: Contains the toolbar settings

Tag: custom/portal/toolbar/mode
Description: The toolbar mode
Value: enable|disable
Default value: enable

Tag: custom/portal/toolbar/prompt-box-title
Description: The universal prompt box title
Value: arbitrary string
Default value: "Address"
Tag: custom/portal/toolbar/browse-button-text
Description: The browse button text
Value: arbitrary string
Default value: "Browse"

Tag: custom/portal/toolbar/logout-prompt-text
Description: The logout prompt text
Value: arbitrary string
Default value: "Logout"

*******************************************************

Tag: custom/portal/column (multiple)
Description: Contains settings of the home page column(s)

Tag: custom/portal/column/order
Description: The order the column from left to right.Columns with lesser order values go
first
Value: arbitrary number
Default value: 0

Tag: custom/portal/column/width
Description: The home page column width
Value: percent
Default value: default value set by browser
Note: The actual width may be increased by browser to accommodate content


*******************************************************


Tag: custom/portal/url-lists
Description: Contains settings for URL lists on the home page

Tag: custom/portal/url-lists/mode
Description: Specifies how to display URL lists on the home page:
             group URL lists by application (group) or
```

```
              show individual URL lists (nogroup).
              URL lists fill out cells of the configured columns, which are not taken
              by custom panes.
              Use the attribute value "nodisplay" to not show URL lists on the home page.

Value: group|nogroup|nodisplay
Default value: group
*******************************************************

Tag: custom/portal/pane (multiple)
Description: Contains settings of the custom pane on the home page

Tag: custom/portal/pane/mode
Description: The mode of the pane
Value: enable|disable
Default value: disable

Tag: custom/portal/pane/title
Description: The title of the pane
Value: arbitrary string
Default value: empty string

Tag: custom/portal/pane/notitle
Description: Hides pane's title bar
Value: yes|no
Default value: no

Tag: custom/portal/pane/type
Description: The type of the pane.Supported types:
              TEXT - inline arbitrary text, may contain HTML tags;
              HTML - HTML content specified by URL shown in the individual iframe;
              IMAGE - image specified by URL
              RSS - RSS feed specified by URL
Value: TEXT|HTML|IMAGE|RSS
Default value: TEXT

Tag: custom/portal/pane/url
Description: The URL for panes with type  HTML,IMAGE or RSS
Value: URL string
Default value: empty string

Tag: custom/portal/pane/text
Description: The text value for panes with type TEXT
Value: arbitrary string
Default value:empty string

Tag: custom/portal/pane/column
Description: The column where the pane located.
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/row
Description: The row where the pane is located
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/height
Description: The height of the pane
Value: number of pixels
Default value: default value set by browser


*******************************************************
```

```
Tag: custom/portal/browse-network-title
Description: The title of the browse network link
Value: arbitrary string
Default value: Browse Entire Network


Tag: custom/portal/access-network-title
Description: The title of the link to start a network access session
Value: arbitrary string
Default value: Start AnyConnect

-->
- <custom>
- <localization>
<languages>en,ja,zh,ru,ua</languages>
<default-language>en</default-language>
</localization>
- <auth-page>
- <window>
- <title-text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</title-text>
</window>
- <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
- <language>
<code>en</code>
<text>English</text>
</language>
- <language>
<code>zh</code>
<text>??(Chinese)</text>
</language>
- <language>
<code>ja</code>
<text>??(Japanese)</text>
</language>
- <language>
<code>ru</code>
<text>???????(Russian)</text>
</language>
- <language>
<code>ua</code>
<text>??????????(Ukrainian)</text>
</language>
</language-selector>
- <logon-form>
- <title-text l10n="yes">
- <![CDATA[
Login
]]>
</title-text>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
```

```
</title-font-color>
- <message-text l10n="yes">
- <![CDATA[
Please enter your username and password.
]]>
</message-text>
- <username-prompt-text l10n="yes">
- <![CDATA[
USERNAME:
]]>
</username-prompt-text>
- <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:
]]>
</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
- <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:
]]>
</group-prompt-text>
- <submit-button-text l10n="yes">
- <![CDATA[
Login
]]>
</submit-button-text>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
- <logout-form>
- <title-text l10n="yes">
- <![CDATA[
Logout
]]>
</title-text>
- <message-text l10n="yes">
- <![CDATA[
Goodbye.
]]>
</message-text>
</logout-form>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
```

```
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
- <info-panel>
<mode>disable</mode>
<image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
- <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
</auth-page>
- <portal>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
```

```
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
- <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
- <application>
<mode>enable</mode>
<id>web-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Web Applications
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks
]]>
</url-list-title>
<order>2</order>
</application>
- <application>
<mode>enable</mode>
<id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks
]]>
</url-list-title>
<order>3</order>
</application>
- <application>
<mode>enable</mode>
<id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access
]]>
</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>net-access</id>
<tab-title l10n="yes">AnyConnect</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>help</id>
<tab-title l10n="yes">Help</tab-title>
<order>1000000</order>
</application>
- <toolbar>
<mode>enable</mode>
<logout-prompt-text l10n="yes">Logout</logout-prompt-text>
<prompt-box-title l10n="yes">Address</prompt-box-title>
<browse-button-text l10n="yes">Browse</browse-button-text>
```

```
</toolbar>
- <column>
<width>100%</width>
<order>1</order>
</column>
- <pane>
<type>TEXT</type>
<mode>disable</mode>
<title />
<text />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>IMAGE</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>HTML</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>RSS</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <url-lists>
<mode>group</mode>
</url-lists>
</portal>
</custom>
```

ヘルプのカスタマイズ

ASA は、クライアントレス セッションの間、アプリケーション ペインにヘルプ コンテンツを表示します。それぞれのクライアントレス アプリケーション ペインには、事前設定されたファイル名を使用する独自のヘルプ ファイルのコンテンツが表示されます。たとえば、[Application Access] パネルに表示されるヘルプ コンテンツは、app-access-hlp.inc というファイルの内容です。表 17-2 に、クライアントレス アプリケーション パネルと、ヘルプのコンテンツの事前設定されたファイル名を示します。

表 17-2　クライアントレス アプリケーション

アプリケーション タイプ	パネル	ファイル名
標準	Application Access	app-access-hlp.inc
標準	Browse Networks	file-access-hlp.inc
標準	AnyConnect Client	net-access-hlp.inc
標準	Web Access	web-access-hlp.inc
プラグイン	MetaFrame Access	ica-hlp.inc
プラグイン	Terminal Servers	rdp-hlp.inc
プラグイン	Telnet/SSH Servers[1]	ssh,telnet-hlp.inc
プラグイン	VNC Connections	vnc-hlp.inc

1. このプラグインは、sshv1 と sshv2 の両方を実行できます。

シスコが提供するヘルプ ファイルをカスタマイズするか、または別の言語でヘルプ ファイルを作成できます。次に [Import] ボタンを使用して、ASA のフラッシュ メモリにそれらのファイルをコピーし、その後のクライアントレス セッション中に表示します。また、以前にインポートしたヘルプ コンテンツ ファイルをエクスポートし、カスタマイズして、フラッシュ メモリに再インポートすることもできます。

ステップ 1　[Import] をクリックして、[Import Application Help Content] ダイアログを起動します。このダイアログでは、クライアントレス セッション中に表示する新しいヘルプ コンテンツをフラッシュ メモリにインポートできます。

ステップ 2　（オプション）[Export] をクリックして、テーブルから選択し、以前にインポートしたヘルプ コンテンツを取得します。

ステップ 3　（オプション）[Delete] をクリックして、テーブルから選択し、以前にインポートしたヘルプ コンテンツを削除します。

ステップ 4　ブラウザに表示される言語の省略形が表示されます。このフィールドは、ファイル変換には*使用されません*。ファイル内で使用される言語を示します。テーブル内の略語に関連付ける言語名を特定するには、ブラウザで表示される言語のリストを表示します。たとえば、次の手順のいずれかを使用すると、ダイアログ ウィンドウに言語と関連の言語コードが表示されます。

- Internet Explorer を起動して、[Tools] > [Internet Options] > [Languages] > [Add] を選択します。
- Mozilla Firefox を起動して、[Tools] > [Options] > [Advanced] > [General] を選択し、[Languages] の隣にある [Choose] をクリックして、[Select a language to add] をクリックします。

ヘルプ コンテンツ ファイルがインポートされたときのファイル名が表示されます。

シスコが提供するヘルプ ファイルのカスタマイズ

シスコが提供するヘルプ ファイルをカスタマイズするには、まず、フラッシュ メモリ カードからファイルのコピーを取得する必要があります。

ステップ 1　ブラウザを使用して、ASA とのクライアントレス セッションを確立します。

ステップ 2　表 17-3 の「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」にある文字列を ASA のアドレスに追加し、次の説明に従って *language* の部分を置き換え、次に Enter を押してヘルプ ファイルを表示します。

表 17-3　クライアントレス アプリケーション用にシスコが提供するヘルプ ファイル

アプリケーション タイプ	パネル	セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL
標準	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc
標準	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc
標準	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc
標準	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc
プラグイン	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc
プラグイン	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc
プラグイン	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc

language は、ブラウザで表示される言語の略語です。略語はファイル変換では*使用されません*。これは、ファイルで使用される言語を示します。シスコが提供する英語版のヘルプ ファイルを表示する場合は、略語として **en** と入力します。

次のアドレス例は、Terminal Servers のヘルプの英語版を表示します。

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

ステップ 3　[File] > [Save (Page) As] を選択します。

（注）　[File name] ボックスの内容は変更しないでください。

ステップ 4　[Save as type] オプションを [Web Page, HTML only] に変更して、[Save] をクリックします。

ステップ 5　任意の HTML エディタを使用してファイルをカスタマイズします。

（注）　ほとんどの HTML タグを使用できますが、文書およびその構造を定義するタグは*使用しないでください*（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグや、コンテンツの構造を決める <p>、<ol>、<ul>、および <li> タグは使用できます。

ステップ 6　オリジナルのファイル名と拡張子を指定して、HTML only としてファイルを保存します。

ステップ 7　ファイル名が表 17-4 にあるファイル名のいずれかと一致すること、および余分なファイル拡張子がないことを確認します。

ASDM に戻り、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Help Customization] > [Import] を選択して、修正されたヘルプ ファイルをフラッシュ メモリにインポートします。

シスコが提供していない言語用のヘルプ ファイルの作成

標準 HTML を使用して他の言語のヘルプ ファイルを作成します。サポートするそれぞれの言語に別のフォルダを作成することをお勧めします。

（注）　ほとんどの HTML タグを使用できますが、文書およびその構造を定義するタグは*使用しないでください*（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグや、コンテンツの構造を決める <p>、<ol>、<ul>、および <li> タグは使用できます。

HTML only としてファイルを保存します。[Filename] カラムにあるファイル名を使用してください。

ASDM に戻り、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Help Customization] > [Import] を選択して、新しいヘルプ ファイルをフラッシュ メモリにインポートします。

アプリケーションのヘルプ コンテンツのインポートおよびエクスポート

[Import Application Help Content] ダイアログボックスを使用して、クライアントレス セッション中にポータル ページに表示するために、ヘルプ ファイルをフラッシュ メモリにインポートします。[Export Application Help Content] ダイアログボックスを使用して、以前にインポートしたヘルプ ファイルをその後の編集のために取得します。

ステップ 1　[Language] フィールドによってブラウザに表示される言語が指定されますが、このフィールドはファイル変換には使用されません （このフィールドは、[Export Application Help Content] ダイアログボックスでは非アクティブです）。[Language] フィールドの横にあるドット（複数）をクリックし、[Browse Language Code] ダイアログボックスで、表示される言語を含む行をダブルクリックします。[Language Code] フィールドの略語がその行の略語と一致することを確認して、[OK] をクリックします。

ステップ 2　ヘルプ コンテンツを提供する言語が [Browse Language Code] ダイアログボックスにない場合は、次の手順を実行します。

1. ブラウザに表示される言語および略語のリストを表示します。
2. 言語の略語を [Language Code] フィールドに入力し、[OK] をクリックします。

   または

   ドット（複数）の左にある [Language] テキスト ボックスに入力することもできます。

次のいずれかの操作を実行すると、ダイアログボックスに言語および関連付けられた言語コードが表示されます。

- Internet Explorer を起動して、[Tools] > [Internet Options] > [Languages] > [Add] を選択します。
- Mozilla Firefox を起動して、[Tools] > [Options] > [Advanced] > [General] を選択し、[Languages] の隣にある [Choose] をクリックして、[Select a language to add] をクリックします。

ステップ 3　インポートしている場合は、新しいヘルプ コンテンツ ファイルを [File Name] ドロップダウン リストから選択します。エクスポートする場合は、このフィールドは使用できません。

ステップ 4　ソース ファイル（インポートの場合）または転送先ファイル（エクスポートの場合）のパラメータを設定します。

- [Local computer]：ソースまたは転送先ファイルがローカル コンピュータにある場合に指定します。
  - [Path]：ソースまたは転送先ファイルのパスを指定します。
  - [Browse Local Files]：ソースまたは転送先ファイルのローカル コンピュータを参照します。
- [Flash file system]：ソースまたは転送先ファイルが ASA のフラッシュ メモリにある場合に指定します。
  - [Path]：フラッシュ メモリ内のソースまたは転送先ファイルのパスを指定します。
  - [Browse Flash]：ソースまたは転送先ファイルのあるフラッシュ メモリを参照します。
- [Remote server]：ソースまたは転送先ファイルがリモート サーバにある場合に指定します。
  - [Path]：ftp、tftp、または http（インポートの場合のみ）の中からファイル転送（コピー）方式を選択し、パスを指定します。

シスコが提供するヘルプ ファイルのカスタマイズ

シスコが提供するヘルプ ファイルをカスタマイズするには、まず、フラッシュ メモリ カードからファイルのコピーを取得する必要があります。

ステップ 1　ブラウザを使用して、ASA とのクライアントレス セッションを確立します。

ステップ 2　表 17-4 の「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」にある文字列を ASA のアドレスに追加し、次の説明に従って *language* の部分を置き換え、次に Enter を押してヘルプ ファイルを表示します。

表 17-4　クライアントレス アプリケーション用にシスコが提供するヘルプ ファイル

アプリケーション タイプ	パネル	セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL
標準	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc
標準	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc
標準	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc
標準	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc
プラグイン	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc
プラグイン	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc
プラグイン	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc

language は、ブラウザで表示される言語の略語です。略語はファイル変換では*使用されません*。これは、ファイルで使用される言語を示します。シスコが提供する英語版のヘルプ ファイルを表示する場合は、略語として **en** と入力します。

次のアドレス例は、Terminal Servers のヘルプの英語版を表示します。

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

ステップ 3　[File] > [Save (Page) As] を選択します。

（注）　[File name] ボックスの内容は変更しないでください。

ステップ 4　[Save as type] オプションを [Web Page, HTML only] に変更して、[Save] をクリックします。

ステップ 5　任意の HTML エディタを使用してファイルをカスタマイズします。

（注）　ほとんどの HTML タグを使用できますが、文書およびその構造を定義するタグは*使用しないでください*（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグや、コンテンツの構造を決める <p>、<ol>、<ul>、および <li> タグは使用できます。

ステップ 6　オリジナルのファイル名と拡張子を指定して、HTML only としてファイルを保存します。

ステップ 7　ファイル名が表 17-4 にあるファイル名のいずれかと一致すること、および余分なファイル拡張子がないことを確認します。

ASDM に戻り、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Help Customization] > [Import] を選択して、修正されたヘルプ ファイルをフラッシュ メモリにインポートします。

シスコが提供していない言語用のヘルプ ファイルの作成

標準 HTML を使用して他の言語のヘルプ ファイルを作成します。サポートするそれぞれの言語に別のフォルダを作成することをお勧めします。

（注）　ほとんどの HTML タグを使用できますが、文書およびその構造を定義するタグは*使用しないでください*（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグや、コンテンツの構造を決める <p>、<ol>、<ul>、および <li> タグは使用できます。

HTML only としてファイルを保存します。表 17-5 のファイル名列にあるファイル名を使用してください。

ASDM に戻り、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Help Customization] > [Import] を選択して、新しいヘルプ ファイルをフラッシュ メモリにインポートします。

ブックマーク ヘルプのカスタマイズ

ASA は、選択した各ブックマークのアプリケーション パネルにヘルプの内容を表示します。これらのヘルプ ファイルをカスタマイズしたり、他の言語でヘルプ ファイルを作成したりできます。次に、後続のセッション中に表示するために、ファイルをフラッシュ メモリにインポートします。事前にインポートしたヘルプ コンテンツ ファイルを取得して、変更し、フラッシュ メモリに再インポートすることもできます。

各アプリケーションのパネルには、事前に設定されたファイル名を使用して独自のヘルプ ファイル コンテンツが表示されます。今後、各ファイルは、ASA のフラッシュ メモリ内の /+CSCOE+/help/*language*/ という URL に置かれます。表 17-5 に、VPN セッション用に保守できる各ヘルプ ファイルの詳細を示します。

表 17-5　VPN アプリケーションのヘルプ ファイル

アプリケーション タイプ	パネル	セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL	シスコが提供するヘルプ ファイルに英語版があるか
標準	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc	Yes
標準	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc	Yes
標準	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc	Yes
標準	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc	Yes
プラグイン	MetaFrame Access	/+CSCOE+/help/*language*/ica-hlp.inc	No
プラグイン	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc	Yes
プラグイン	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc	Yes
プラグイン	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc	Yes

language は、ブラウザに表示される言語の省略形です。このフィールドは、ファイル変換には*使用されません*。ファイル内で使用される言語を示します。特定の言語コードを指定するには、ブラウザに表示される言語のリストからその言語の省略形をコピーします。たとえば、次の手順のいずれかを使用すると、ダイアログ ウィンドウに言語と関連の言語コードが表示されます。

- Internet Explorer を起動して、[Tools] > [Internet Options] > [Languages] > [Add] を選択します。
- Mozilla Firefox を起動して、[Tools] > [Options] > [Advanced] > [General] を選択し、[Languages] の隣にある [Choose] をクリックして、[Select a language to add] をクリックします。

シスコが提供するヘルプ ファイルのカスタマイズ

シスコが提供するヘルプ ファイルをカスタマイズするには、まずフラッシュ メモリ カードからファイルのコピーを取得する必要があります。次の手順で、コピーを取得してカスタマイズします。

ステップ 1　ブラウザを使用して、ASA とのクライアントレス SSL VPN セッションを確立します。

ステップ 2　表 17-5 の「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」にある文字列を ASA のアドレスに追加し、Enter を押してヘルプ ファイルを表示します。

（注）　英語版のヘルプ ファイルを取得するには、**language** のところに *en* を入力します。

次のアドレス例は、Terminal Servers のヘルプの英語版を表示します。

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

ステップ 3　[File] > [Save (Page) As] を選択します。

（注）　[File name] ボックスの内容は変更しないでください。

ステップ 4　[Save as type] オプションを [Web Page, HTML only] に変更して、[Save] をクリックします。

ステップ 5　任意の HTML エディタを使用してファイルを変更します。

（注）　ほとんどの HTML タグを使用できますが、文書およびその構造を定義するタグは*使用しないでください*（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグや、コンテンツの構造を決める <p>、<ol>、<ul>、および <li> タグは使用できます。

ステップ 6　オリジナルのファイル名と拡張子を指定して、HTML only としてファイルを保存します。

ステップ 7　ファイル名が表 17-5 にあるファイル名のいずれかと一致すること、および余分なファイル拡張子がないことを確認します。

ASDM に戻り、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Help Customization] > [Import] を選択して、新しいヘルプ ファイルをフラッシュ メモリにインポートします。

シスコが提供していない言語用のヘルプ ファイルの作成

HTML を使用して、他の言語でヘルプ ファイルを作成します。

サポートするそれぞれの言語に別のフォルダを作成することをお勧めします。

HTML only としてファイルを保存します。表 17-5 の「セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL」の最後のスラッシュの後にあるファイル名を使用します。

VPN セッション中に表示するためにファイルをインポートする場合は、次の項を参照してください。

制約事項

ほとんどの HTML タグを使用できますが、文書およびその構造を定義するタグは*使用しないでください*（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグや、コンテンツの構造を決める <p>、<ol>、<ul>、および <li> タグは使用できます。

言語変換について

ASA は、クライアントレス SSL VPN セッション全体の言語変換を提供します。これには、ログイン、ログアウト バナー、およびプラグインおよび AnyConnect などの認証後に表示されるポータル ページが含まれます。リモート ユーザに可視である機能エリアとそれらのメッセージは、変換ドメイン内にまとめられています。表 17-6 に、変換ドメインと変換される機能エリアを示します。

表 17-6　言語変換ドメインのオプション

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN クライアントのユーザ インターフェイスに表示されるメッセージ。
banners	クライアントレス接続で VPN アクセスが拒否される場合に表示されるメッセージ。

変換ドメイン	変換される機能エリア
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-rdp2	Java Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。
PortForwarder	ポート フォワーディング ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。

ASA には、標準機能の一部である各ドメイン用の変換テーブル テンプレートが含まれています。プラグインのテンプレートはプラグインとともに含まれており、独自の変換ドメインを定義します。

変換ドメインのテンプレートをエクスポートできます。これで、入力する URL にテンプレートの XML ファイルが作成されます。このファイルのメッセージ フィールドは空です。メッセージを編集して、テンプレートをインポートし、フラッシュ メモリに置かれる新しい変換テーブル オブジェクトを作成できます。

既存の変換テーブルをエクスポートすることもできます。作成した XML ファイルに事前に編集したメッセージが表示されます。この XML ファイルを同じ言語名で再インポートすると、新しいバージョンの変換テーブルが作成され、以前のメッセージが上書きされます。

テンプレートにはスタティックのものも、ASA の設定に基づいて変化するものもあります。*クライアントレス ユーザのログインおよびログアウト ページ*、*ポータル ページ*、*および URL ブックマーク*はカスタマイズが可能なため、ASA は **customization** および **url-list** 変換ドメイン テンプレートをダイナミックに生成し、テンプレートは変更内容をこれらの機能エリアに自動的に反映させます。

変換テーブルを作成した後、このテーブルを使用して、カスタマイゼーション オブジェクトを作成し、グループ ポリシーまたはユーザ属性に適用できます。AnyConnect 変換ドメイン以外では、カスタマイゼーション オブジェクトを作成し、そのオブジェクトで使用する変換テーブルを識別し、グループ ポリシーまたはユーザに対してそのカスタマイゼーションを指定するまで、変換テーブルは影響を及ぼすことはなく、ユーザ画面のメッセージは変換されません。AnyConnect ドメインの変換テーブルに対する変更は、ただちに AnyConnect クライアント ユーザに表示されます。

変換テーブルの編集

ステップ 1　[Configuration] > [Remote Access VPN] > [Language Localization] の順に進みます。[Language Localization] ペインが表示されたら、[Add] をクリックします。

ステップ 2　ドロップダウン ボックスから言語ローカリゼーション テンプレートを選択します。このボックスのエントリは、変換する機能エリアに対応します。

ステップ 3　テンプレートの言語を指定します。テンプレートはキャッシュ メモリ内の変換テーブルになり、指定した名前が付きます。ブラウザの言語オプションと互換性のある短縮形を使用してください。たとえば、中国語のテーブルを作成するときに IE を使用している場合は、IE によって認識される *zh* という略語を使用します。

ステップ 4　変換テーブルを編集します。msgid フィールドで表される変換対象のメッセージごとに、対応する msgstr フィールドの引用符の間に変換済みテキストを入力します。次の例では、メッセージ Connected の msgstr フィールドにスペイン語テキストを入力しています。

```
msgid "Connected"
msgstr "Conectado"
```

ステップ 5　[OK] をクリックします。

変換テーブルの追加

テンプレートに基づいて新しい変換テーブルを追加するか、またはこのペインですでにインポートされた変換テーブルを修正できます。

ステップ 1　修正するテンプレートを選択し、新しい変換テーブルの基礎として使用します。テンプレートは変換ドメインに構成され、特定の機能領域に影響します。表 17-6 に、変換ドメインと影響を受ける機能エリアを示します （このフィールドは [GUI Text and Messages] ペインにグレー表示されます）。

ステップ 2　ドロップダウン リストから変換ドメインを選択します （このフィールドは [GUI Text and Messages] ペインにグレー表示されます）。

ステップ 3　言語を指定します。ブラウザの言語オプションと互換性のある略語を使用してください。ASA は、この名前で新しい変換テーブルを作成します。

ステップ 4　エディタを使用してメッセージ変換を変更します。メッセージ ID フィールド（msgid）には、デフォルトの変換が含まれています。msgid に続くメッセージ文字列フィールド（msgstr）で変換を指定します。変換を作成するには、msgstr 文字列の引用符の間に変換対象のテキストを入力します。たとえば、「Connected」というメッセージをスペイン語に変換するには、msgstr の引用符の間にスペイン語のテキストを挿入します。

```
msgid "Connected"
msgstr "Conectado"
```

変更を行った後、[Apply] をクリックして変換テーブルをインポートします。

クライアントレス SSL VPN のトラブルシューティング

hosts ファイル エラーを回避するための Application Access の終了

Application Access の実行の妨げになる hosts ファイル エラーを回避するために、Application Access を使用し終えたら、Application Access ウィンドウを必ず閉じるようにします。ウィンドウを閉じるには、[Close] アイコンをクリックします。

Application Access 使用時の hosts ファイル エラーからの回復

Application Access ウィンドウを正しく閉じないと、次のエラーが発生する可能性があります。

- 次に Application Access を起動しようとしたときに、Application Access がオフに切り替わっている可能性があり、「`Backup HOSTS File Found`」エラー メッセージが表示される。
- アプリケーションをローカルで実行している場合でも、アプリケーション自体がオフに切り替わっているか、または動作しない。

このようなエラーは、Application Access ウィンドウを不適切な方法で終了したことが原因です。次に例を示します。

- Application Access の使用中に、ブラウザがクラッシュした。
- Application Access の使用中に、停電またはシステム シャットダウンが発生した。
- 作業中に Application Access ウィンドウを最小化し、このウィンドウがアクティブな状態（ただし最小化されている）でコンピュータをシャットダウンした。

- 「hosts ファイルの概要」
- 「不正な Application Access の終了」
- 「クライアントレス SSL VPN による hosts ファイルの自動再設定」
- 「手動による hosts ファイルの再設定」

hosts ファイルの概要

ローカル システム上の hosts ファイルは、IP アドレスをホスト名にマッピングしています。Application Access を起動すると、クライアントレス SSL VPN は hosts ファイルを修正し、クライアントレス SSL VPN 固有のエントリを追加します。Application Access ウィンドウを正しく閉じて Application Access を終了すると、hosts ファイルは元の状態に戻ります。

Application Access の起動前	hosts ファイルは元の状態です。
Application Access の起動時	• クライアントレス SSL VPN は hosts ファイルを hosts.webvpn にコピーして、バックアップを作成します。 • 次に、クライアントレス SSL VPN は hosts ファイルを編集し、クライアントレス SSL VPN 固有の情報を挿入します。
Application Access の終了時	• クライアントレス SSL VPN はバックアップ ファイルを hosts ファイルにコピーして、hosts ファイルを元の状態に戻します。 • クライアントレス SSL VPN は、hosts.webvpn を削除します。
Application Access の終了後	hosts ファイルは元の状態です。

（注）　Microsoft 社のアンチスパイウェア ソフトウェアは、ポート転送 Java アプレットによる hosts ファイルの変更をブロックします。アンチスパイウェア ソフトウェアの使用時に hosts ファイルの変更を許可する方法の詳細については、www.microsoft.com を参照してください。

不正な Application Access の終了

Application Access が正しく終了しなかった場合は、hosts ファイルは、クライアントレス SSL VPN 用にカスタマイズされた状態のままになっています。ユーザが次に Application Access を起動するときに、クライアントレス SSL VPN は hosts.webvpn ファイルを検索することで、Application Access の状態をチェックします。hosts.webvpn ファイルが検出されると、「Backup HOSTS File Found」というエラー メッセージが表示され（図 18-1 を参照）、Application Access が一時的にオフに切り替わります。

Application Access を正しくシャットダウンしないと、リモート アクセス クライアント/サーバ アプリケーションが不安定な状態のままになります。クライアントレス SSL VPN を使用せずにこれらのアプリケーションを起動しようとすると、正しく動作しない場合があります。通常の接続先のホストが使用できなくなる場合があります。一般にこのような状況は、自宅からリモートでアプリケーションを実行し、Application Access ウィンドウを終了せずにコンピュータをシャットダウンし、その後職場でそのアプリケーションを実行しようとした場合に発生します。

クライアントレス SSL VPN による hosts ファイルの自動再設定

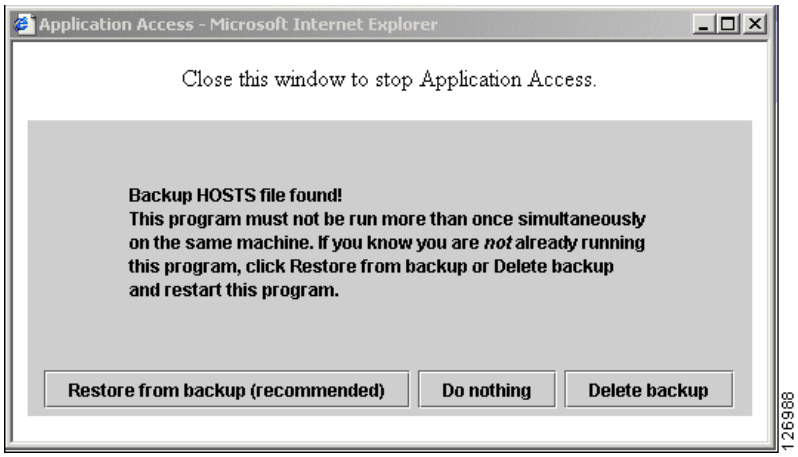
リモート アクセス サーバに接続できる場合は、hosts ファイルを再設定し、Application Access やアプリケーションを再度イネーブルにするために、次の手順を実行します。

手順の詳細

ステップ 1　クライアントレス SSL VPN を起動してログインします。ホームページが開きます。

ステップ 2　[Applications Access] リンクをクリックします。`Backup HOSTS File Found` メッセージが表示されます （図 18-1 を参照）。

図 18-1　Backup HOSTS File Found メッセージ



ステップ 3　次のいずれかのオプションを選択します。

- [Restore from backup] : クライアントレス SSL VPN は強制的に正しくシャットダウンされます。クライアントレス SSL VPN は hosts.webvpn backup ファイルを `hosts` ファイルにコピーし、hosts ファイルを元の状態に戻してから、hosts.webvpn を削除します。その後、Application Access を再起動する必要があります。
- [Do nothing] : Application Access は起動しません。リモート アクセスのホームページが再び表示されます。
- [Delete backup] : クライアントレス SSL VPN は hosts.webvpn ファイルを削除し、hosts ファイルをクライアントレス SSL VPN 用にカスタマイズされた状態にしておきます。元の `hosts` ファイル設定は失われます。Application Access は、クライアントレス SSL VPN 用にカスタマイズされた hosts ファイルを新しいオリジナルとして使用して起動します。このオプションは、hosts ファイル設定が失われても問題がない場合にだけ選択してください。Application Access が不適切にシャットダウンされた後に、ユーザまたはユーザが使用するプログラムによって hosts ファイルが編集された可能性がある場合は、他の 2 つのオプションのどちらかを選択するか、または hosts ファイルを手動で編集します（「手動による hosts ファイルの再設定」を参照）。

手動による hosts ファイルの再設定

現在の場所からリモート アクセス サーバに接続できない場合や、カスタマイズした hosts ファイルの編集内容を失いたくない場合は、次の手順に従って、hosts ファイルを再設定し、Application Access とアプリケーションを再度イネーブルにします。

手順の詳細

ステップ 1　hosts ファイルを見つけて編集します。最も一般的な場所は、c:\windows\sysem32\drivers\etc\hosts です。

ステップ 2　`# added by WebVpnPortForward` という文字列が含まれている行があるかどうかをチェックします。この文字列を含む行がある場合、hosts ファイルはクライアントレス SSL VPN 用にカスタマイズされています。hosts ファイルがクライアントレス SSL VPN 用にカスタマイズされている場合、次の例のようになっています。

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# これは、Microsoft TCP/IP for Windows が使用する hosts ファイルのサンプルです。
#
# このファイルには、ホスト名に対する IP アドレスのマッピングが含まれています。Each
# エントリは個別の行に納める必要があります。IP アドレスは
# 最初のカラムに配置し、その後ろに対応するホスト名を続けてください。
# IP アドレスとホスト名は 1 以上のスペースで区切る
# 必要があります。
#
# さらに、コメント（たとえば、この文）は、「#」記号で示した個別の行に挿入するか、
# またはマシン名を続けます。
#
# 例：
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

ステップ 3　`# added by WebVpnPortForward` という文字列が含まれている行を削除します。

ステップ 4　ファイルを保存して、閉じます。

ステップ 5　クライアントレス SSL VPN を起動してログインします。

ホームページが表示されます。

ステップ 6　[Application Access] リンクをクリックします。

[Application Access] ウィンドウが表示されます。これで Application Access がイネーブルになります。

管理者によるクライアントレス SSL VPN ユーザへのアラート送信

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Administrator's Alert Message to Clientless SSL VPN Users] の順に選択します。

[Administrator's Alert Message to Clientless SSL VPN Users] ダイアログボックスが表示されます。

ステップ 2　送信する新規または編集済みのアラート内容を入力して、[Post Alert] をクリックします。

ステップ 3　現在のアラート内容を削除して新しいアラート内容を入力するには、[Cancel Alert] をクリックします。

CHAPTER 19

クライアントレス SSL VPN ライセンス

ライセンス

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件
ASA 5506-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • Security Plus ライセンス：4 セッション。*オプションの SSL VPN ライセンス：10 セッション。* *共有ライセンスはサポートされていません。*
ASA 5512-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5515-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5525-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*

モデル	ライセンス要件
ASA 5545-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5555-X	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5585-X（SSP-10）	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASA 5585-X（SSP-20、-40、および -60）	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASASM	AnyConnect Premium ライセンス： • 基本ライセンス：2 セッション。 • *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* • *オプションの共有ライセンス：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。*
ASAv5	標準ライセンス：250 セッション。
ASAv10	• 標準ライセンス：（9.3(1)）2 セッション。（9.3(2)）250 セッション。 • Premium ライセンス：250 セッション。
ASAv30	• 標準ライセンス：（9.3(1)）2 セッション。（9.3(2)）750 セッション。 • Premium ライセンス：750 セッション。

クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアントセッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を越えることはできません。

（AnyConnect 4 以降）：同時ユーザ数および VPN 機能数は、別途入手可能な AnyConnect ライセンスによって制御されます。VPN ライセンスは、ASA における最大レベルまで有効になります。

（AnyConnect 3 以前）：共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。