ASDM における VPN 設定手順の概要
Version 5.2(1)

Text Part Number: OL-10670-01-J

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

以下の情報は Class A 装置の FCC 適合に関するものです。この装置はテスト済みであり、FCC ルールの Part 15 に記載されている Class A デジタル装置の制限に準拠していることが確認済みです。この制限により、Class A デジタル装置を商業施設で作動させた場合、有害な干渉が起きないようになっています。この装置は、無線周波エネルギーを発生、使用し、また放射することもあります。取り扱い説明書に従って設置または使用しなかった場合には、無線通信に有害な干渉を起こすことがあります。また、この装置を住居で使用する場合には有害な干渉を起こすことがあり、ユーザ側の費用で干渉防止措置を講じなければならない場合があります。

以下の情報は Class B 装置の FCC 適合に関するものです。このマニュアルで解説している装置は、無線周波エネルギーを発生し、また放射することもあります。シスコのインストレーションに関する指示に従って設置されない場合には、ラジオやテレビの受信に干渉を起こす可能性があります。この装置は、テスト済みであり、FCC ルールの Part 15 に記載されている仕様に基づく Class B デジタル装置の制限に準拠していることが確認済みです。この仕様では、住居に設置した場合にこのような干渉が起きないようになっています。ただし、特定の設置条件で干渉が起きないことを保証するものではありません。

シスコによる書面での認可なしに装置に対して変更を行うと、Class A または Class B デジタル装置に要求される FCC への適合ができない可能性があります。この場合、装置の使用権限は FCC 規制によって制限され、ユーザ側の費用でラジオまたはテレビへの干渉防止措置を講じなければならない場合があります。

装置の電源を切ることによって、装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコの装置またはその周辺装置が原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

・干渉がなくなるまでテレビまたはラジオのアンテナの向きを変えます。

・テレビまたはラジオの左右どちらかの側に装置を移動します。

・テレビまたはラジオから離れた場所に装置を移動します。

・テレビまたはラジオとは別の回路にあるコンセントに装置を接続します（装置とテレビ / ラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

シスコより認められていない変更をこの製品に対して行った場合には、FCC 認定が無効になり、さらに製品を操作するユーザの権限を失うことになります。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）パブリック ドメイン バージョンとして、UCB が開発したプログラムを最適化したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

このドキュメントで使用しているインターネット プロトコル（IP）アドレスは、実在のアドレスではありません。ドキュメント中で示される例、コマンドの画面出力、および図は、いずれも視覚的な説明のみを目的としています。実在する IP アドレスが例示されていた場合、それらは意図して使用したものではありません。

ASDM における VPN 設定手順の概要 Version 5.2(1)

CONTENTS

このマニュアルについて

このマニュアルでは、適用型セキュリティ アプライアンスにおける ASDM による VPN 機能の設定手順について説明します。

対象読者

このマニュアルは、Adaptive Security Device Manager を使用し、バーチャル プライベート ネットワークの ASA のセットアップや設定を行うシステムエンジニア（SE）および ネットワーク管理者を対象としています。読者は、ネットワーク機器、基本的なネットワークの概念、およびバーチャル プライベート ネットワークについて理解している必要があります。

マニュアルの構成

このマニュアルの構成は、次の通りです。

章番号	説明
第 1 章「デジタル証明書の登録」	デジタル証明書の登録、鍵ペアの生成、トラストポイントの生成、および証明書を取得する SCEP の使用について説明しています。
第 2 章「グループ ポリシーの設定」	グループ ポリシーの設定について説明しています。グループ ポリシーとトンネル グループ および ユーザの関連について説明しています。
第 3 章「SVC の設定」	VPN トンネル テクノロジーである SVC の設定について説明しています。これによって、ネットワーク管理者がリモート コンピュータへの IPSec VPN クライアントをインストールして設定しなくても、リモート ユーザは IPSec VPN クライアントの利点を利用できます。
第 4 章「Windows クライアントと VPN 3002　クライアントのクライアント アップデートの設定」	クライアント アップデートの設定方法について説明しています。これによって、中心的な場所にいる管理者が、VPN クライアント ユーザに VPN クライアント ソフトウェア および VPN 3002 ハードウェア クライアント イメージをアップデートする時期にあることを自動的に通知することができます。
第 5 章「DDNS アップデートの設定」	ダイナミック DNS リソース レコードをアップデートする DHCP サーバの設定方法について説明しています。
第 6 章「LDAP AAA サーバの設定」	セキュリティ アプライアンスと同じ内部ネットワークにある Microsoft Active Directory Server（LDAP）を使用して、セキュリティ アプライアンスのユーザ認証および認可を設定する手順の例を紹介しています。
第 7 章「Citrix MetaFrame サービスの設定」	Citrix MetaFrame サービスをサポートするセキュリティ アプライアンスの設定について説明しています。この場合の証明書の設定方法も示しています。
第 8 章「WebVPN に対する SSO の設定」	SSO について説明しています。これによって、WebVPN ユーザは、ユーザ名とパスワードを一度だけ入力して複数の保護されたサービスおよび Web サーバにアクセスできます。Siteminder SSO および HTTP Form プロトコルを設定する手順についても説明しています。
第 9 章「ネットワーク アドミッション コントロールの設定」	Network Admission Control（NAC; ネットワーク アドミッション コントロール）の設定について説明しています。これによって、実稼働環境でのネットワーク アクセスの条件として、エンドポイントの準拠性と脆弱性のチェックを実行し、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や感染から企業ネットワークを保護します。
第 10 章「L2TP over IPSec の設定」	セキュリティ アプライアンスの設定について説明します。これによって、リモート Windows クライアントが、Layer 2 Tunneling Protocol（L2TP）を使用して、パブリック IP ネットワークへアクセスし、プライベートおよび会社のネットワーク サーバと安全に通信できます。

章番号	説明
第 11 章「ロード バランシングの設定」	ロード バランシングの概念および ASA 5520 以降のモデルへのロード バランシングの設定方法について説明しています。
第 12 章「ASA 5505 での Easy VPN Services の設定」	ASA 5505 における VPN サービスの設定方法について説明しています。これによって、ハードウェア クライアントまたはヘッドエンドとして実行できますが、両方同時には実行できません。

関連マニュアル

このマニュアルは、次のユーザ ガイドと一緒に利用することができます。

- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Migrating to ASA 7.1(1) from the VPN 3000 Series Concentrator*
- *Release Notes for Cisco Secure Desktop*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

表記法

このマニュアルは、次の表記法を使用しています。

表記法	説明
太字	ユーザアクションおよびコマンドは、太字で示しています。
イタリック体	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。
screen 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、screen フォントで示しています。
太字の **screen** フォント	入力する必要のある情報は、コマンド ライン インターフェイスの **boldface screen** フォントで示しています（たとえば、**vpnclient stat**）。

（注）は、次の表記法を使用しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次の表記法を使用しています。

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。

システムを設定および管理する際、指示がある場合を除き、次のようにデータを入力してください。

データのタイプ	形式
IP アドレス	IP アドレスの表記には、4 バイトのドット付き 10 進法による表記法（たとえば、192.168.12.34）を使用してください。例で示すように、先頭の 0 を省略することができます。
サブネット マスクおよびワイルドカード マスク	サブネット マスクは、4 バイトのドット付き 10 進法による表記法（たとえば、255.255.255.0）を使用します。ワイルドカード マスクも、同じ表記法を使用します（たとえば、0.0.0.255）。例で示すように、先頭の 0 を省略することができます。
MAC アドレス	MAC アドレスは、6 バイトの 16 進数による表記法（たとえば、0001.03cf.0238）を使用します。
ホスト名	ホスト名は、正当なネットワーク ホスト名または、エンドシステム名による表記法（たとえば、VPN01）を使用します。スペースは、使用できません。ホスト名は、ネットワーク上の特定のシステムを一意に識別する必要があります。
文字列	文字列は、大文字および小文字の英数字を使用します。ほとんどの文字列は、大文字と小文字を区別します（たとえば、simon および Simon は、異なるユーザ名を示します）。通常、文字列の最大長は 48 文字です。
ポート番号	ポート番号は、0 から 65535 の 10 進数を使用します。番号中に、カンマやスペースは使用できません。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

シスコの最新のマニュアルには、次の URL からアクセスできます。

http://www.cisco.com/univercd/home/home.htm

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering ツールからシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support Web サイト

Cisco Technical Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコの TAC エンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/servicerequest

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- 『*Cisco Product Catalog*』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『*Cisco Product Catalog*』には、次の URL からアクセスしてください。

  http://cisco.com/univercd/cc/td/doc/pcat/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新のオンライン情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

デジタル証明書の登録

この章では、ASDM を使用してデジタル証明書を登録する方法について説明します。登録が完了すると、その証明書を使用して VPN の LAN 間トンネルおよびリモート アクセス トンネルを認証できます。認証に事前共有鍵だけを使用する場合は、この章を読む必要はありません。

この章には、次の項があります。

（注） この章の手順の実行中に、ASDM ウィンドウに表示されるアトリビュートの詳細を参照するには、**Help** をクリックしてください。

設定手順の概要

CA を登録し、トンネルを認証するための ID 証明書を取得するには、次のタスクを実行します。

(注)　この例では、自動（SCEP）登録を示します。

1. ID 証明書の鍵ペアを作成します。この鍵ペアは、RSA 鍵です。次の項の手順では、RSA 鍵ペアを生成する方法を説明します。
2. トラストポイントを作成します。この例では、トラストポイントの名前は newmsroot です。
3. 登録 URL を設定します。この例で使用している URL は、http://10.20.30.40/certsrv/mscep/mscep.dll です。
4. CA を認証します。
5. CA を登録し、ID 証明書を ASA 上に取得します。

鍵ペアについて

各ピアには、公開鍵と秘密鍵の両方を含む鍵ペアが 1 つあります。これらの鍵は補完的に動作します。一方の鍵で暗号化された通信は、もう一方の鍵で復号化されます。

鍵ペアは、RSA 鍵です。

- 鍵の最大モジュラスは 2048 で、デフォルトのサイズは 1024 ビットです。
- シグニチャ操作の場合、鍵の最大サイズは 4096 ビットです。
- 署名と暗号化の両方に使用できる汎用の RSA 鍵ペアを生成できます。*特定用途向けの* RSA 鍵ペアの場合は、それぞれの目的に応じて分かれるため、対応する ID ごとに 2 つの証明書が必要です。デフォルトの設定は、汎用です。

証明書に鍵ペアを設定するには、生成する鍵ペアを識別するラベルを指定します。次の項では、ASDM を使用して指定のラベル付きの RSA 鍵ペアを生成する方法、およびその他のパラメータのデフォルト設定を使用する方法を説明します。

RSA 鍵ペアの生成

RSA 鍵ペアを生成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Key Pair** ウィンドウで、**Add** をクリックします。

ステップ 2　**Add Key Pair** ダイアログボックスで情報を設定します。

a. **Name**：デフォルト名を使用する場合はクリックします。または、鍵ペアの名前を入力します。この例では、デフォルトの RSA 鍵を使用しますが、代わりに key1 などの名前を入力できます。

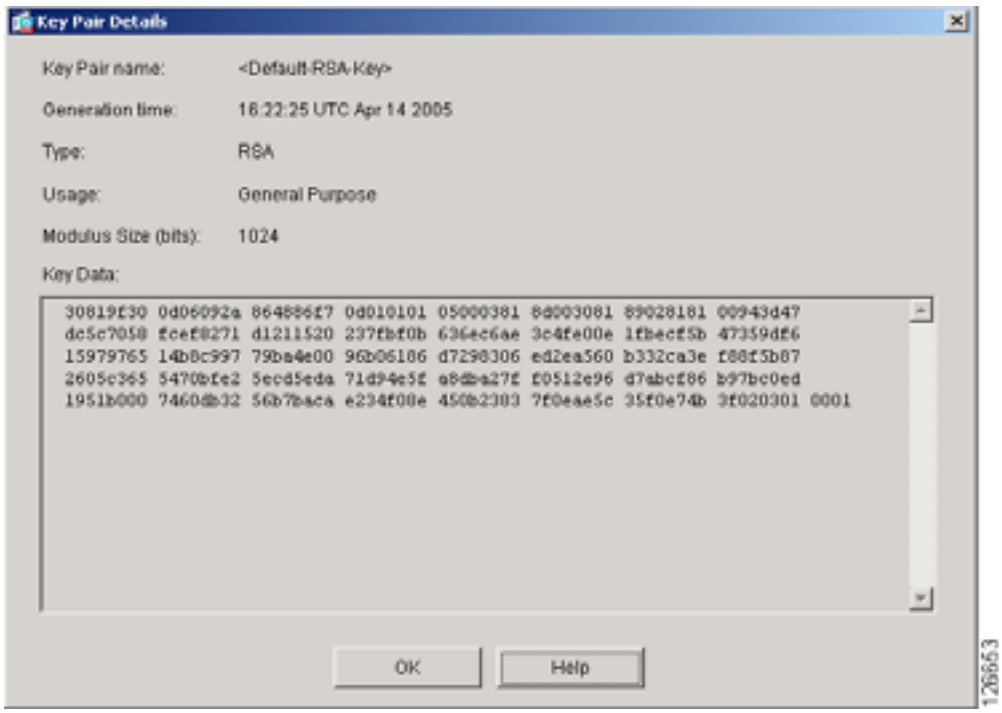
b. **Size** リスト：RSA 鍵ペアの場合、**Size** リストには、オプションとして 512、768、1024、または 2048 が表示されます。デフォルト サイズは 1024 です。この例では、デフォルト設定を受け入れます。

c. **Usage** オプション：オプションは、General Purpose（署名および暗号化の両方に 1 つのペアを使用）と Special（機能ごとに 1 つのペアを使用）です。この例では、デフォルト設定（General Purpose）を受け入れます。

ステップ 3　**Generate Now** をクリックします。

ステップ 4　生成された鍵ペアを表示するには、**Show Details** をクリックします。ASDM に、鍵ペアに関する情報が表示されます。図 1-1 に出力例を示します。

図 1-1　鍵ペアの詳細表示



トラストポイントの作成

トラストポイントは CA と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションを含んでいます。トラストポイントを作成するには、使用するインターフェイスの名前の項を参照してください。

トラストポイントを作成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Trustpoint > Configuration** ウィンドウで、**Add** をクリックします。

ステップ 2　**Add Trustpoint Configuration** ダイアログボックスで、基本情報を設定します。その他のすべてのパラメータについては、デフォルト値を受け入れます。

a. **Trustpoint Name** フィールド：**Trustpoint Name** フィールドにトラストポイントの名前を入力します。この例では、名前は newmsroot です。

b. **Enrollment URL** フィールド：**Enrollment Settings** ウィンドウの **Enrollment Mode** 領域で、**Use automatic enrollment** オプションをオンにします。次に、このフィールドに登録 URL を入力します。この例では、**10.20.30.40/certsrv/mscep/mscep.dll** と入力します。

ステップ 3　Common Name（CN; 通常名）と Organizational Unit（OU; 組織ユニット）の名前を使用して、サブジェクト名を設定します。

a. **Enrollment Settings** ウィンドウの **Key Pair** リストから、このトラストポイントに対して設定した鍵ペアを選択します。この例では、鍵ペアは key1 です。

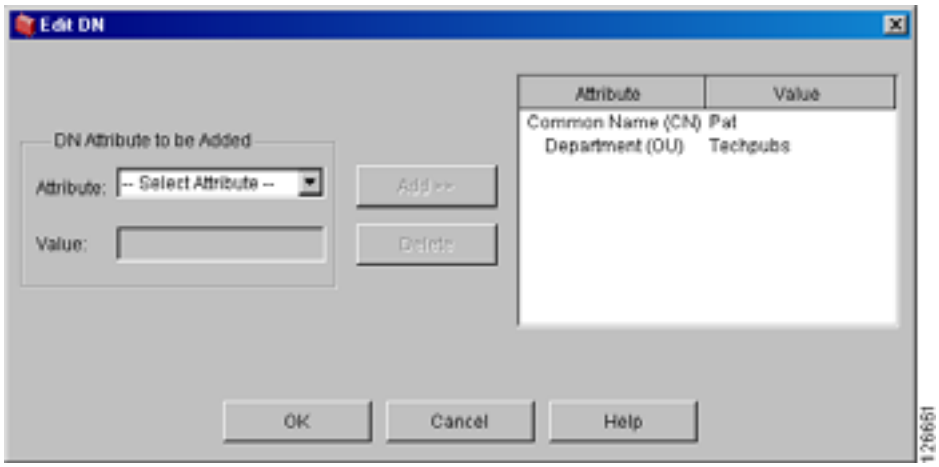
b. **Enrollment Settings** ウィンドウで、**Certificate Parameters** をクリックします。

c. サブジェクト識別名（X.500）の値を追加するには、**Certificate Parameters** ダイアログボックスで **Edit** をクリックします。

d. **Edit DN** 領域で、**DN Attribute to be Added** の下にある **Attribute** リストからアトリビュートを選択し、**Value** フィールドに値を入力します。次に **Add** をクリックします。DN 情報を入力したら、**OK** をクリックします。

この例では、まず **Common Name (CN)** を選択し、**Value** フィールドに **Pat** と入力します。次に Add をクリックしてから、**Department (OU)** を選択して、**Value** フィールドに **Techpubs** と入力します。図 1-2 は、**Edit DN** ダイアログボックスに入力した内容を示しています。

図 1-2　サブジェクト名のアトリビュートと値



ステップ 4　ダイアログボックスを確認したら、**OK** をクリックして、残りの 2 つのダイアログボックスで **OK** をクリックします。

SCEP による証明書の取得

この項では、SCEP を使用して証明書を設定する方法を説明します。自動登録の場合は、設定するトラストポイントごとに手順を繰り返します。各トラストポイントに対する手順が完了すると、セキュリティ アプライアンスは CA 証明書をトラストポイント用に 1 つ、署名および暗号化用に 1 つまたは 2 つを受信します。これらの手順を実行しない場合、セキュリティ アプライアンスによって Base 64 形式の CA 証明書をテキストボックスに貼り付けるよう求められます。

汎用の RSA 鍵を使用する場合、受信した証明書は署名と暗号化を目的としたものです。署名と暗号化に別個の RSA 鍵を使用すると、セキュリティ アプライアンスは目的ごとに別個の証明書を受信します。

証明書を取得するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Authentication** ウィンドウを選択します。

ステップ 2　**Trustpoint Name** リストで、トラストポイントの名前を選択します。この例では、**newmsroot** を選択します。

ステップ 3　**Authenticate** をクリックします。

ステップ 4　**Apply** をクリックします。ASDM で **Authentication Successful** ダイアログが表示されたら、**OK** をクリックします。

認証局への登録

トラストポイントを設定して認証したら、次の手順を実行して ID 証明書を登録できます。

ステップ 1　**Configuration > Properties > Certificate > Enrollment** ウィンドウで、**Trustpoint Name** リストからトラストポイントを選択します。この例では、**newmsroot** を選択します。

ステップ 2　**Enroll** をクリックします。

証明書の管理

証明書を管理するには、**Configuration > Properties > Certificate > Manage Certificates** ウィンドウを使用します。

このウィンドウを使用して、新しい証明書の追加や証明書の削除を行うことができます。

このペインには、次の情報が表示されます。

- Subject：証明書の所有者を特定します。
- Type：CA、RA 全般、RA 暗号化、RA シグニチャ、ID
- Status：Available または Pending
  - Available は、CA が登録要求を受け入れて、ID 証明書を発行したことを意味します。
  - Pending は、登録要求が処理中であるため、CA が ID 証明書をまだ発行していないことを意味します。
- Usage：証明書が使用される方法（シグニチャ、汎用、または暗号化）を特定します。

Show Details をクリックして、証明書に関する情報も表示できます。Certificate Details ダイアログには、3 つのテーブル（General、Subject、および Issuer）が表示されます。

General：タイプ、シリアル番号、ステータス、使用方法、CRL 分散ポイント、証明書の有効期間、および関連付けられたトラストポイントの値を表示します。これは、Available および Pending ステータスの両方に適用されます。

Subject：サブジェクト DN または証明書所有者の X.500 フィールドと値を表示します。これは、Available ステータスだけに適用されます。

Issuer：証明書を付与したエンティティの X.500 フィールドを表示します。これは、Available ステータスだけに適用されます。

CHAPTER 2

グループ ポリシーの設定

この章では、ASDM を使用して VPN グループ ポリシーを設定する方法について説明します。この章には、次の項があります。

グループ、グループ ポリシー、トンネル グループ、およびユーザは、相互に依存しています。要約すると、まずトンネル グループを設定し、接続の値を設定します。次に、グループ ポリシーを設定します。これによって、集約的にユーザに値が設定されます。次に、ユーザを設定します。ユーザはグループから値を継承することも、ユーザごとに特定の値を設定することもできます。この章では、グループ ポリシーを設定する方法と目的について説明します。

グループ ポリシー、トンネル グループ、ユーザの概要

この章ではグループ ポリシーだけを扱いますが、これらのグループ ポリシーが存在するコンテキストを理解する必要があります。グループとユーザは、virtual private network（VPN; バーチャル プライベート ネットワーク）のセキュリティ管理およびセキュリティ アプライアンスの設定における中心的な概念です。これらは、ユーザの VPN へのアクセス権および VPN の使用方法を定義するアトリビュートを指定します。*グループ*は、単一エンティティとして扱われるユーザの集合です。*ユーザ*は自分のアトリビュートを*グループ ポリシー*から取得します。*トンネル グループ*は、特定の接続のグループ ポリシーを識別します。ユーザに特定のグループ ポリシーを割り当てない場合、接続のデフォルト グループ ポリシーが適用されます。

トンネル グループとグループ ポリシーを使用すると、システム管理が簡素化されます。設定タスクを効率化するために、セキュリティ アプライアンスには、デフォルト LAN 間トンネル グループ、デフォルト リモート アクセス トンネル グループ、デフォルト WebVPN トンネル グループ、およびデフォルト グループ ポリシー（DfltGrpPolicy）が用意されています。デフォルト トンネル グループとグループ ポリシーによって、多くのユーザに共通であると考えられる設定を提供します。ユーザを追加するときに、グループ ポリシーからパラメータを「継承」するように指定できます。これによって、大量のユーザの VPN アクセスを簡単に設定できます。

すべての VPN ユーザに同一の権限を与える場合は、特定のトンネル グループまたはグループ ポリシーを設定する必要はありませんが、そのような場合はほとんどありません。たとえば、財務グループがプライベート ネットワークの一部にアクセスできるようにして、カスタマー サポート グループが別の部分に、MIS グループがさらに別の部分にアクセスできるようにすることがあります。また、MIS の特定のユーザが、他の MIS ユーザがアクセスできないシステムにアクセスできるようにすることもあります。トンネル グループおよびグループ ポリシーは、このような処理を安全に行う柔軟性を提供します。

（注） セキュリティ アプライアンスには、ネットワーク リストのスーパーセットであるオブジェクト グループの概念も含まれています。オブジェクト グループを使用すると、ポートやネットワークへの VPN アクセスを定義できます。オブジェクト グループは、グループ ポリシーおよびトンネル グループではなく、ACL に関連します。オブジェクト グループの使用の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の第 16 章「Identifying Traffic with Access Lists」を参照してください。

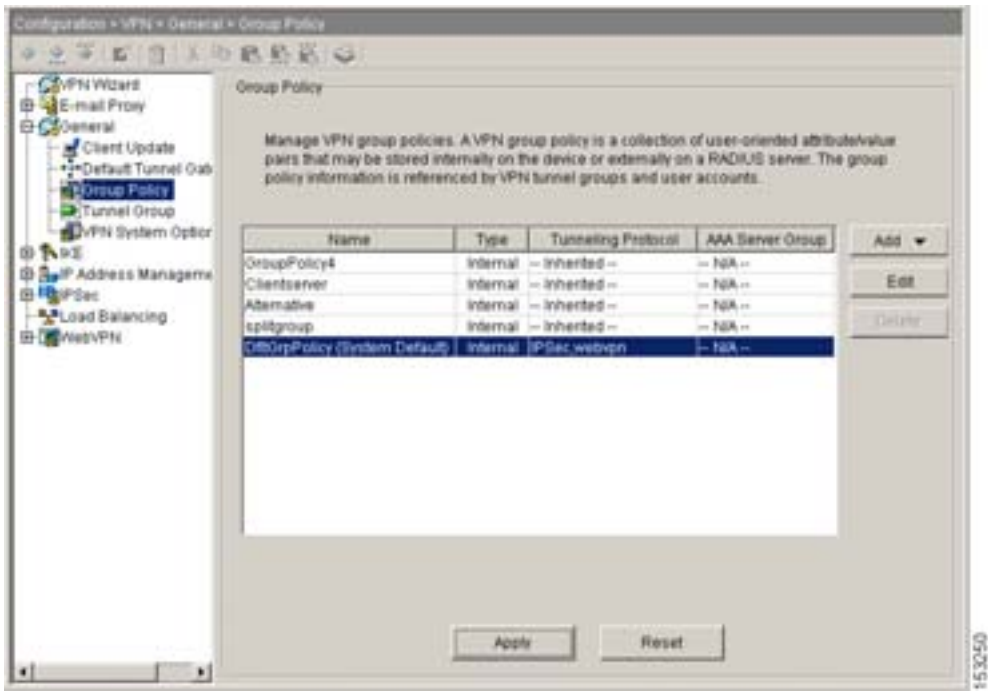
グループ ポリシー

グループ ポリシーを使用すると、ユーザごとに個別に各アトリビュートを指定するのではなく、アトリビュートのセット全体をユーザまたはユーザのグループに適用できます。また、特定のユーザのグループ ポリシー アトリビュートを修正できます。

グループ ポリシーは、デバイスの内部（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 IPSec 接続に関するユーザ指向のアトリビュートと値のペアのセットです。トンネル グループは、トンネルが確立された後、ユーザ接続の期間を設定するグループ ポリシーを使用します。

グループ ポリシーのユーザへの割り当てまたは特定のユーザのグループ ポリシーの修正を行うには、**Configuration > VPN > General > Group Policy** を選択します（図 2-1）。

図 2-1　Group Policy ウィンドウ



内部および外部グループ ポリシーを設定できます。内部グループは、セキュリティ アプライアンスの内部データベースに設定されます。外部グループは、RADIUS や LDAP などの外部認証サーバに設定されます。グループ ポリシーには、次のアトリビュートが含まれます。

- ID
- サーバ定義
- クライアント ファイアウォールの設定
- トンネリング プロトコル
- IPSec 設定
- ハードウェア クライアント設定
- フィルタ
- クライアント設定の設定値
- ネットワーク アドミッション コントロールの設定値
- WebVPN 機能
- 接続設定

デフォルトのグループ ポリシー

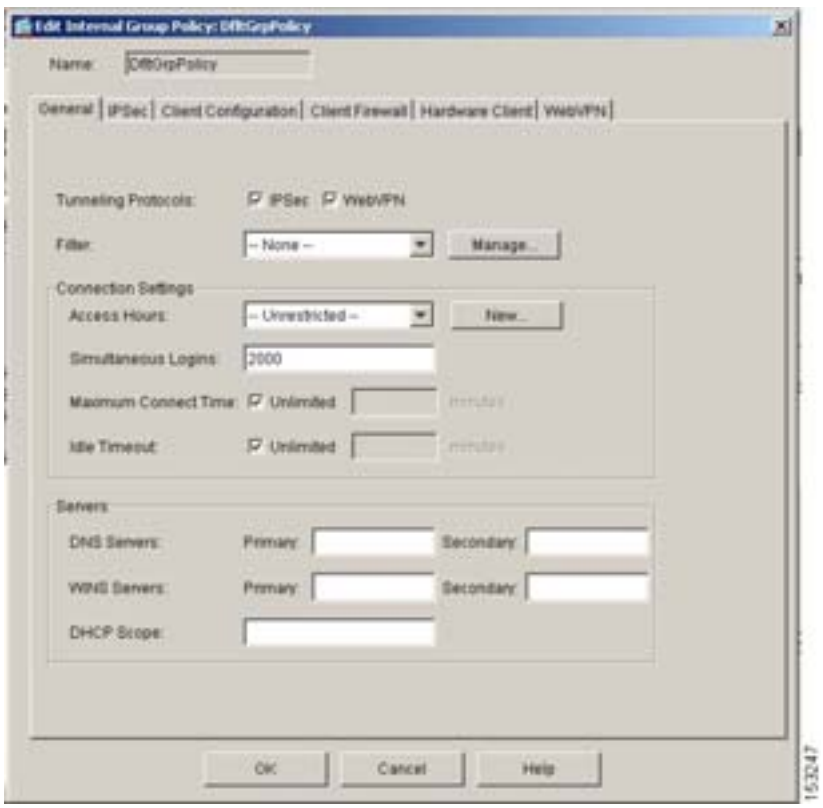
セキュリティ アプライアンスには、セキュリティ アプライアンスに常に存在する DfltGrpPolicy というデフォルト グループ ポリシーが用意されています。このデフォルト グループ ポリシーは、セキュリティ アプライアンスで使用するように設定しない限り、有効になりません。DfltGrpPolicy は、常に内部グループ ポリシーです。このデフォルト グループ ポリシーは修正できますが、削除はできません。他のグループ ポリシーを設定した場合、明示的に指定しなかったアトリビュートは、デフォルト グループ ポリシーから値が取得されます。

Group Policy ウィンドウを使用して、VPN グループ ポリシーを管理できます。デフォルト VPN グループ ポリシーを設定することによって、個別のグループまたはユーザ名レベルで設定しなかったアトリビュートをユーザが継承するようにできます。デフォルトでは、VPN ユーザにグループ ポリシー アソシエーションはありません。グループ ポリシー情報は、VPN 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。

「子」のウィンドウ、タブ、およびダイアログボックスを使用して、デフォルト グループ パラメータを設定できます。これらのパラメータは、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、これによって設定タスクが効率化されます。グループはデフォルト 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。

デフォルト グループ ポリシーを修正するには、Group Policy ウィンドウのテーブルで DfltGrpPolicy を選択し、**Edit** をクリックします。Edit Internal Group Policy: DfltGrpPolicy ウィンドウが表示されます（図 2-2）。

図 2-2　Edit Internal Group Policy: DfltGrpPolicy ウィンドウ



デフォルト グループ ポリシーのアトリビュートを変更するには、他の内部グループ ポリシーの場合と同様に、Edit Internal Group Policy: DfltGrpPolicy ウィンドウのさまざまなタブで選択を行います。P.2-11 の「内部グループ ポリシーの設定」を参照してください。

セキュリティ アプライアンスのデフォルト グループ ポリシーの DfltGrpPolicy には、次のアトリビュートがあります。

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 wins-server none
 dns-server none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol IPSec
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 banner none
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 leap-bypass disable
 nem disable
 backup-servers keep-client-config
 client-firewall none
 client-access-rule none
 webvpn
  functions url-entry
  no html-content-filter
  no homepage
  no filter
  no url-list
  no port-forward
  port-forward-name value Application Access
```

グループ ポリシーの設定

この項には、次の項があります。

グループ ポリシーは、任意の種類のトンネルに適用できます。どの場合も、明示的にパラメータを定義しない場合、グループはデフォルト グループ ポリシーから値を取得します。グループ ポリシーを設定（追加または修正）するには、次の項の手順に従います。

Add ダイアログボックスをクリックすると、新しい内部グループ ポリシーを作成するか、外部の RADIUS または LDAP サーバに格納される外部グループ ポリシーを作成するかを選択できる小さなメニューが表示されます。Add Internal Group Policy ウィンドウと Edit Group Policy ウィンドウのどちらにも、タブ付きのセクションがあります。WebVPN タブをクリックすると、いくつかの追加のタブが表示されます。それぞれのタブをクリックすると、パラメータが表示されます。タブ間を移動するとき、セキュリティ アプライアンスは新しい設定を保持します。すべてのタブ付きセクションでパラメータの設定を完了したら、OK または Cancel をクリックします。

これらの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。

- 全般的なパラメータ：プロトコル、フィルタリング、接続設定、サーバ
- IPSec パラメータ：IP セキュリティ トンネリング プロトコルのパラメータおよびクライアント アクセス ルール
- クライアント設定パラメータ：バナー、パスワード保管、スプリットトンネリング ポリシー、デフォルト ドメイン名、IPSec over UDP、バックアップ サーバ
- クライアント ファイアウォール パラメータ：VPN クライアント パーソナル ファイアウォールの要件
- ハードウェア クライアント パラメータ：インタラクティブ ハードウェア クライアントおよび個別のユーザ認証、ネットワーク拡張モード
- ネットワーク アドミッション コントロール パラメータ
- WebVPN パラメータ：SSL VPN アクセス

上記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
- ルールとフィルタ
- IPSec セキュリティ アソシエーション
- 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
- ユーザ認証サーバ（特に、内部認証サーバ）

外部グループ ポリシーの設定

外部グループ ポリシーは、指定された外部サーバからアトリビュート値を取得します。外部グループ ポリシーでは、セキュリティ アプライアンスがアトリビュートを問い合せることができる AAA サーバ グループを識別し、外部 AAA サーバ グループからアトリビュートを取得するときに使用するパスワードを指定する必要があります。外部認証サーバを使用し、認証しようとするユーザと同じ RADIUS サーバに外部グループポリシー アトリビュートが存在する場合は、両者の間に名前の重複がないことを確認する必要があります。

(注) セキュリティ アプライアンスの外部グループ名は、RADIUS サーバのユーザ名を参照します。つまり、セキュリティ アプライアンスで外部グループ X を設定すると、RADIUS サーバは、この問い合せをユーザ X の認証要求と見なします。そのため、外部グループは、セキュリティ アプライアンスにとって特別な意味を持つ RADIUS サーバ上のユーザ アカウントになります。認証しようとするユーザと同じ RADIUS サーバに外部グループ アトリビュートが存在する場合、両者の間で名前の重複があってはいけません。

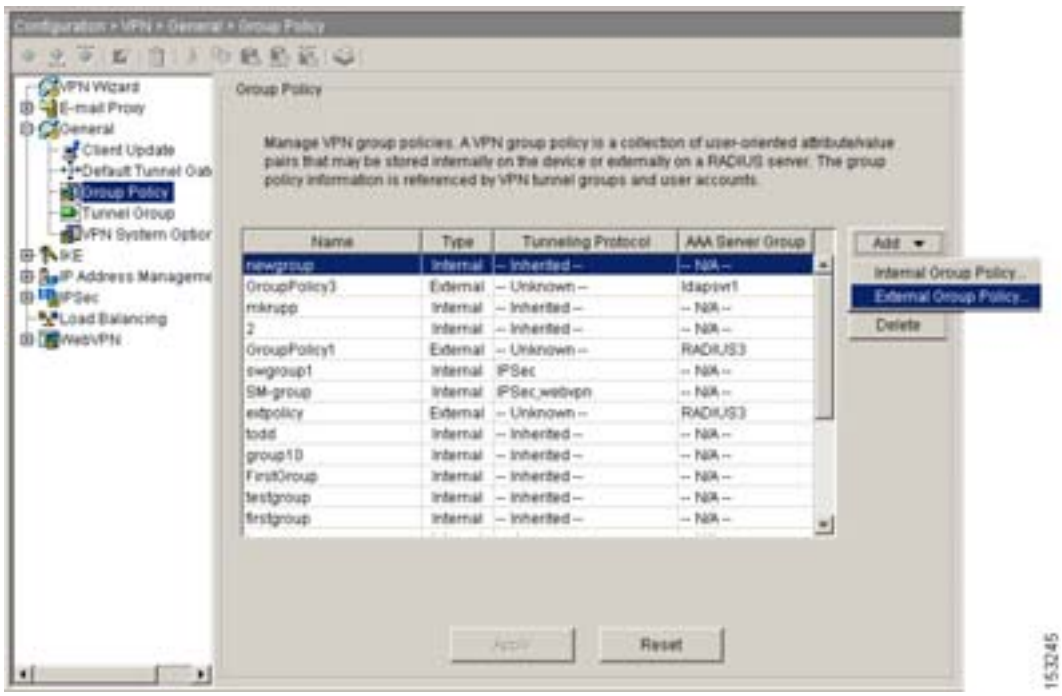
セキュリティ アプライアンスは、外部 LDAP または RADIUS サーバでのユーザ認証をサポートします。外部サーバを使用するようにセキュリティ アプライアンスを設定する前に、正しいセキュリティ アプライアンス認証アトリビュートでサーバを設定し、このアトリビュートのサブセットから、個別のユーザに特定の権限を割り当てる必要があります。『*Cisco Security Appliance Command Line Configuration Guide*』の付録 E「Configuring an External Server for Security Appliance User Authorization」の説明に従い、外部サーバを設定します。

外部グループ ポリシーの追加

次の手順で、外部グループ ポリシーの追加方法について説明します。

ステップ 1　外部グループ ポリシーを追加するには、**Configuration > VPN > General > Group Policy** を選択し、**Add** をクリックして、メニューから **External Group Policy** を選択します（図 2-3）。

図 2-3　外部グループ ポリシーの追加



Add External Group Policy ダイアログボックスが表示されます（図 2-4）。

図 2-4　Add External Group Policy ダイアログボックス

新しい外部グループ ポリシーのアトリビュートを設定するには、次の手順を実行し、グループ ポリシーの名前とタイプ、およびサーバグループ名とパスワードを指定します。

ステップ 2　グループ ポリシーの名前とサーバのパスワードを入力します。次に、リストからサーバ グループを選択するか、New をクリックして新しいサーバ グループを作成します。New をクリックすると、メニューが表示されます。新しい RADIUS サーバ グループまたは新しい LDAP サーバ グループを選択します。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（図 2-5）。終了したら OK をクリックします。

（注）　外部グループ ポリシーでは、RADIUS は AAA サーバ タイプのみサポートされます。

図 2-5　Add AAA Server Group ダイアログボックス

ステップ 3　AAA サーバ グループ パラメータを設定します。Add AAA Server Group ダイアログボックスを使用して、次のアトリビュートで新しい AAA サーバ グループを設定できます。Accounting Mode アトリビュートは、RADIUS および TACACS+ プロトコルにのみ適用されます。

- Server Group：サーバ グループの名前を指定します。新しいサーバ グループの名前を指定して、そのグループにサーバを追加できます。指定したサーバ グループにサーバが含まれていない場合、次のメッセージが表示されます（図 2-6）。

図 2-6　空のサーバ グループのメッセージ

グループにサーバを追加するには、**Configuration > Properties >AAA Setup > AAA Groups** を選択します。このメッセージが表示された後で継続するには、**OK** をクリックします。外部グループ設定の手順を終了するには、**Cancel** をクリックします。

- Protocol：（*表示のみ*）RADIUS サーバ グループか、LDAP サーバ グループかを示します。外部グループ ポリシーでは、常に RADIUS です。
- Accounting Mode：*RADIUS および TACACS+ プロトコルのみ*）同時アカウンティング モードと単一アカウンティング モードのどちらを使用するかを示します。単一モードでは、セキュリティ アプライアンスはアカウンティング データを 1 つのサーバにのみ送信します。同時モードでは、セキュリティ アプライアンスはアカウンティング データをグループ内のすべてのサーバに送信します。
- Reactivation Mode：障害が発生したサーバを再アクティブ化する方法を Depletion または Timed 再アクティブ化モードから指定します。Depletion モードでは、障害が発生したサーバは、グループ内のサーバのすべてが非アクティブになった場合にのみ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 秒の停止時間の後で再アクティブ化されます。
- Dead Time：Depletion モードで、グループの最後のサーバが無効になってから、すべてのサーバを次に再度有効にするまでの経過時間を分単位で指定します。このフィールドは、Timed モードでは使用できません。
- Max Failed Attempts：応答しないサーバが非アクティブであると宣言するまでの失敗接続試行回数を指定します（1 ～ 5 の整数）。

（注） いくつかの vendor-specific attribute（VSA; ベンダー固有属性）は、『*Cisco Security Appliance Command Line Configuration Guide*』の付録 E「Configuring an External Server for Security Appliance User Authorization」で説明するように、設定できます。RADIUS サーバが Class アトリビュート（#25）を返すように設定されている場合、セキュリティ アプライアンスは、このアトリビュートを使用してグループ名を認証します。RADIUS サーバでは、アトリビュートの形式は OU=*groupname* とする必要があります。ここで、*groupname* は、セキュリティ アプライアンスで設定したグループ名です（OU=Finance など）。

外部グループ ポリシーの編集

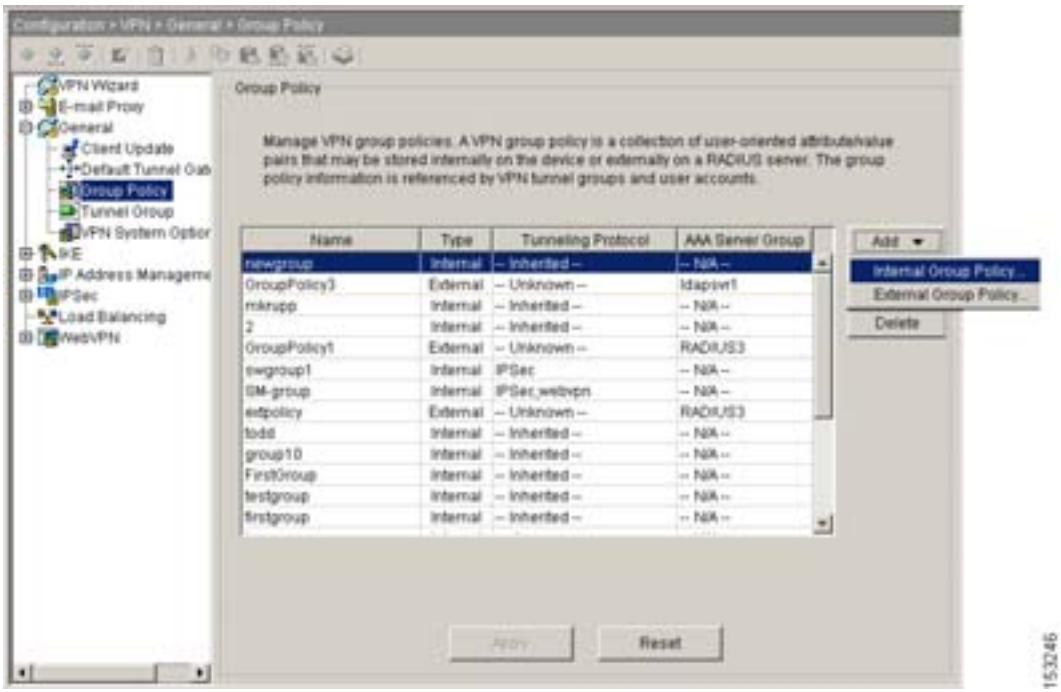
グループ ポリシーの編集手順は追加手順と似ていますが、Group Policy ウィンドウで **Edit** をクリックすると、Edit Group Policy ウィンドウが表示され、Name フィールドにすでに値が入力されているという違いがあります。このウィンドウのその他のフィールドは同じです。外部グループ ポリシーを編集するときに、AAA サーバ グループを追加することもできます。P.2-7 の「外部グループ ポリシーの追加」のステップ 2 および 3 を参照してください。

内部グループ ポリシーの設定

内部グループ ポリシーは、セキュリティ アプライアンスの内部データベースに設定されます。新しい内部グループ ポリシーのアトリビュートを設定するには、次の手順を実行します。

ステップ 1　内部グループ ポリシーを追加または編集するには、**Configuration >VPN > General >Group Policy** を選択します。Group Policy ウィンドウが表示されます（図 2-7）。

図 2-7　Group Policy ウィンドウ（Add Internal Group Policy）

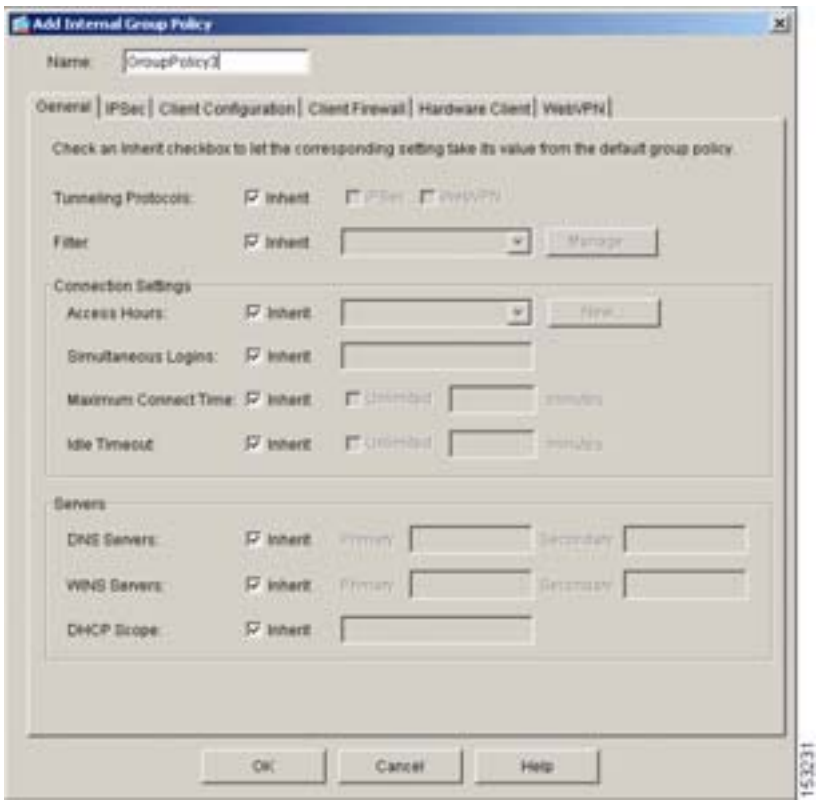


ステップ 2　**Add** または **Edit** をクリックします。

- 内部グループ ポリシーを追加する場合は、メニューから **Internal Group Policy** を選択します。Add Internal Group Policy ウィンドウが表示されます（図 2-8）。
- 内部グループ ポリシーを編集する場合は、Edit Internal Group Policy ウィンドウが表示されます。

これらのウィンドウの内容は似ています。唯一の違いは、編集の場合、Name フィールドが表示専用であることです。このように似ているため、次の手順では、Add Internal Group Policy ウィンドウのみを示します。

図 2-8　Add Internal Group Policy ウィンドウ



このウィンドウには、機能固有のアトリビュートを設定するいくつかのタブがあります。ほとんどの場合、Inherit チェックボックスを選択することで、対応する設定をデフォルト グループ ポリシーから取得できます。継承によって、設定プロセスを大幅に簡素化できます。継承しないアトリビュートは、明示的に設定できます。次の項では、内部グループ ポリシーのグループ ポリシー アトリビュートの設定方法について説明します。

内部グループ ポリシーの全般的なアトリビュートの設定

Add Internal Group Policy ウィンドウまたは Edit Internal Group Policy ウィンドウの General タブを使用して、追加または修正するグループ ポリシーのトンネリング プロトコル、ACL フィルタ、接続設定、およびサーバを設定できます。このウィンドウの各フィールドで、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 チェックボックスをクリアすると、特定の値を設定できます。

次の項では、General タブの各アトリビュートの値の設定方法について説明します。

トンネリング プロトコルの設定

このグループが使用できるトンネリング プロトコルを選択します（複数可）。ユーザは、選択されているプロトコルのみを使用できます。ユーザが VPN トンネルで接続できるようにするには、1 つ以上のトンネリング モードを設定する必要があります。デフォルトは IPSec です。

選択肢は次のとおりです。

- IPSec：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。IPSec は、LAN 間（ピアツーピア）接続と、クライアントと LAN の接続の両方で使用できます。IPSec チェックボックスを選択すると、セキュリティ アプライアンスは 2 つのピア間（リモート アクセス クライアントまたはその他のセキュアなゲートウェイ）で IPSec トンネルをネゴシエートし、認証、暗号化、カプセル化、鍵管理を制御するセキュリティ アソシエーションを作成します。
- WebVPN：SSL/TLS を利用する VPN。WebVPN チェックボックスを選択すると、HTTPS 対応 Web ブラウザ経由でリモート ユーザに VPN サービスが提供されます。クライアント（ハードウェアまたはソフトウェア）は必要ありません。このプロトコルは、Web ブラウザを使用して、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 トンネルを確立します。WebVPN 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。
- L2TP over IPSec：いくつかの一般的な 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、PPP over UDP（ポート 1701）を使用して、データをトンネリングします。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。

（注） プロトコルを選択しなかった場合、エラー メッセージが表示されます。

実行コンフィギュレーションからプロトコル アトリビュートを削除するには、そのプロトコルのチェックボックスをクリアします。

ACL フィルタの設定

フィルタは、セキュリティ アプライアンス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。ACL を設定して、このグループ ポリシーでさまざまなトラフィック タイプを許可または拒否します（このアトリビュートは、ユーザ名モードでも設定できます。その場合、ユーザ名で設定された値がグループ ポリシーの値よりも優先されます）。

（注） セキュリティ アプライアンスは、インターフェイスのインバウンド ACL のみをサポートします。

各 ACL の最後には、access control entry（ACE; アクセス コントロール エントリ）で明示的に許可されないすべてのトラフィックを拒否する、暗黙の表記されないルールが含まれます。このトピックでは、ACE をルールと呼びます。

グループ ポリシーがデフォルト グループ ポリシーからフィルタを継承するように指定するには、Inherit チェックボックスを選択します。これがデフォルト値です。別のフィルタを指定するには、メニューからフィルタを選択します。値の継承を抑止するには、ACL 名を指定する代わりに **None** を選択します。***None*** オプションは、アクセスリストがなく、ヌル値を設定することを示します。その結果、アクセスリストが拒否されます。

(注)　設定の時点では、グループ　ポリシーが継承する値がわからないことがあります。特定のグループ ポリシーに ACL を関連付けないようにするには、Inherit チェックボックスをクリアし、ACL (Filter/Web-VPN ACL ID/...) ドロップダウン リストで **None** を選択します。

デフォルト グループ ポリシーのいずれかを操作する場合は、継承が適用されないため、***None*** を選択するだけで同じ効果が得られます。

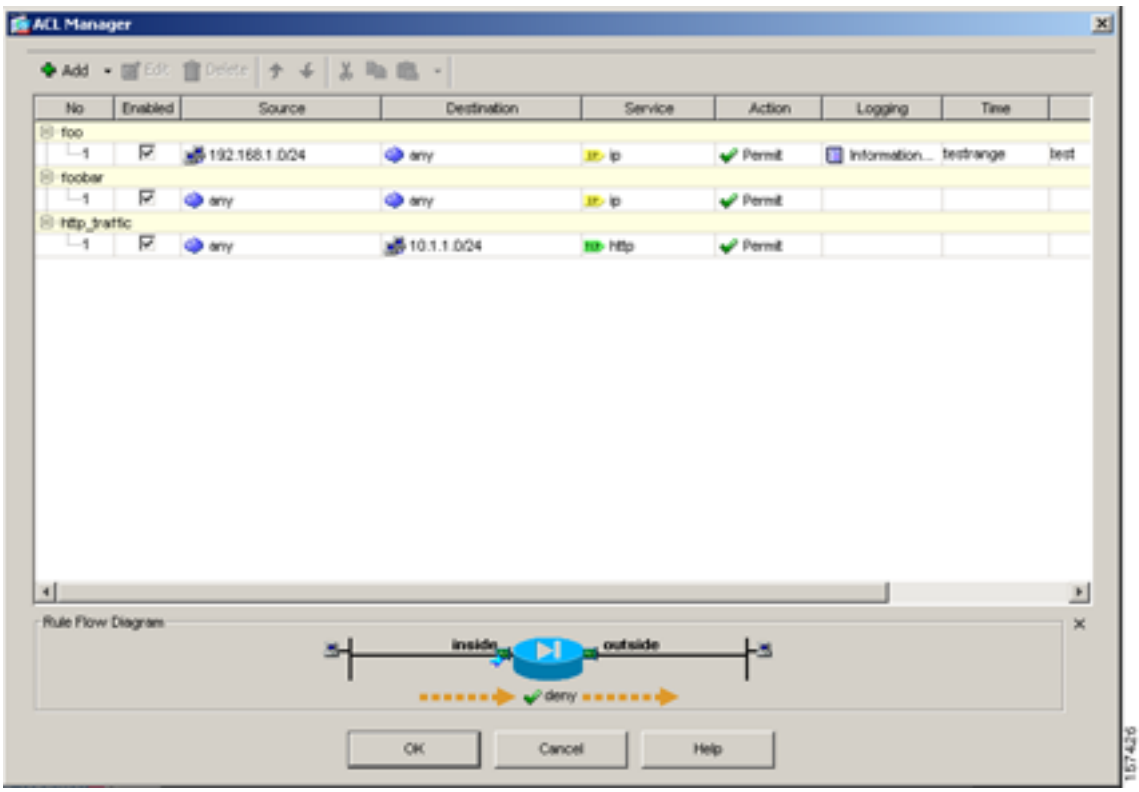
Inherit または None を選択した場合は、既存のフィルタの追加または修正を行わないため、この手順の P.2-25 の「アクセス時間の設定」までスキップできます。

ACL と ACE の管理

新しいフィルタ（ACL）の作成または既存のフィルタの修正を行うには、**Manage** をクリックします。ACL Manager ダイアログボックス（図 2-9）が表示されます。このダイアログボックスで、Access Control List（ACL; アクセス コントロール リスト）および拡張アクセス コントロール リストを追加、編集、削除して、特定のホストまたはネットワークから別のホストまたはネットワークへのアクセス（使用できるプロトコルやポートなど）を制御できます。

グループ ポリシーから ACL を削除するには、ツールバーから **Delete** を選択します。確認されず、やり直しもできません。

図 2-9　ACL Manager ダイアログボックス



このダイアログボックスのフィールドは、次のとおりです。

- No：ルールの評価順序を示します。暗黙のルールには番号が付けられず、ハイフンで表されます。
- Enabled：ルールを有効または無効にします。暗黙のルールは無効にできません。
- Source：Destination カラムにリストされている IP アドレスへのトラフィックの送信を許可または拒否するホストまたはネットワークの IP アドレスが表示されます。アドレス カラムには、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）。これは、内部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。
- Destination：Source Host/Network カラムにリストされている IP アドレスからのトラフィックの受信を許可または拒否するホストまたはネットワークの IP アドレスが表示されます。アドレス カラムには、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）。これは、外部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。アドレス カラムには、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、ファイアウォール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、ファイアウォールはこのアドレス マッピングを維持します。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。ACL で許可されていれば、この時間内に、外部ホストはプールの変換済みアドレスを使用して、内部ホストへの接続を開始できます。通常、内部ホストは常に同じ IP アドレスを使用するため、外部から内部への接続にはスタティック トランスレーションが必要です。
- Service：ルールで指定されるサービスとプロトコルの名前。プロトコルとサービスの詳細については、P.2-19 の「プロトコルおよびサービス グループの管理」を参照してください。
- Action：ルールに適用されるアクションが表示されます（Permit または Deny）。
- Logging：ログレベルと、ログ メッセージ間の間隔（秒単位）が表示されます（ACL のロギングを有効にした場合）。ロギング オプション（ロギングの有効化と無効化を含む）を設定するには、ツールバーから **Edit** を選択します。Edit ACE 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は、タイトル バーを除き、Add ACE ダイアログボックス（図 2-12）と同じです。
- Time：このルールで適用される時間範囲の名前が表示されます。時間範囲は、このグループ ポリシーを使用してユーザが接続できるアクセス時間を指定します。デフォルト値は (any) で、ユーザが接続できる時間に制限がないことを意味します。
- Description：ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule.」という説明が付けられます。説明を編集するには、ツールバーから **Edit** を選択します。Edit ACE 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は、タイトル バーを除き、Add ACE ダイアログボックス（図 2-12）と同じです。
- Rule Flow Diagram：（読み取り専用）選択したルール フローのグラフィカルな表現を表示します。この図を閉じるには、Rule Flow Diagram 領域の上にある小さな「X」をクリックします。画面を明示的に閉じるまで、ACL Manager ダイアログボックスに同じ図が表示されます。

ルールは、ACL Manager ダイアログボックスのテーブルに表示されている順に適用されます。ルールをリストの上または下に移動するには、ツールバーの上矢印または下矢印をクリックします。ルールを削除するには、削除するルールを選択して、**Delete** をクリックします。

ACL および ACE は、テキスト ドキュメントと同様に、ツールバーのはさみ（切り取り）、ページ（コピー）、クリップボード（貼り付け）のアイコンをクリックして、切り取り、コピー、貼り付けができます。

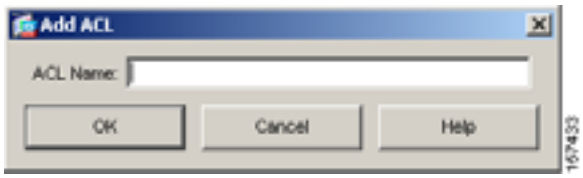
ACL Manager テーブルの任意の行をダブルクリックすると、Edit ACL ダイアログボックスが開き、これらのフィールドを修正できます。

新しい ACL を追加するには、**Add** をクリックし、ドロップダウン リストから **Add ACL** を選択します（図 2-10）。

図 2-10　Add/Insert メニュー

Add ACL ダイアログボックスが表示されます（図 2-11）。ACL 名を入力し、OK をクリックします。

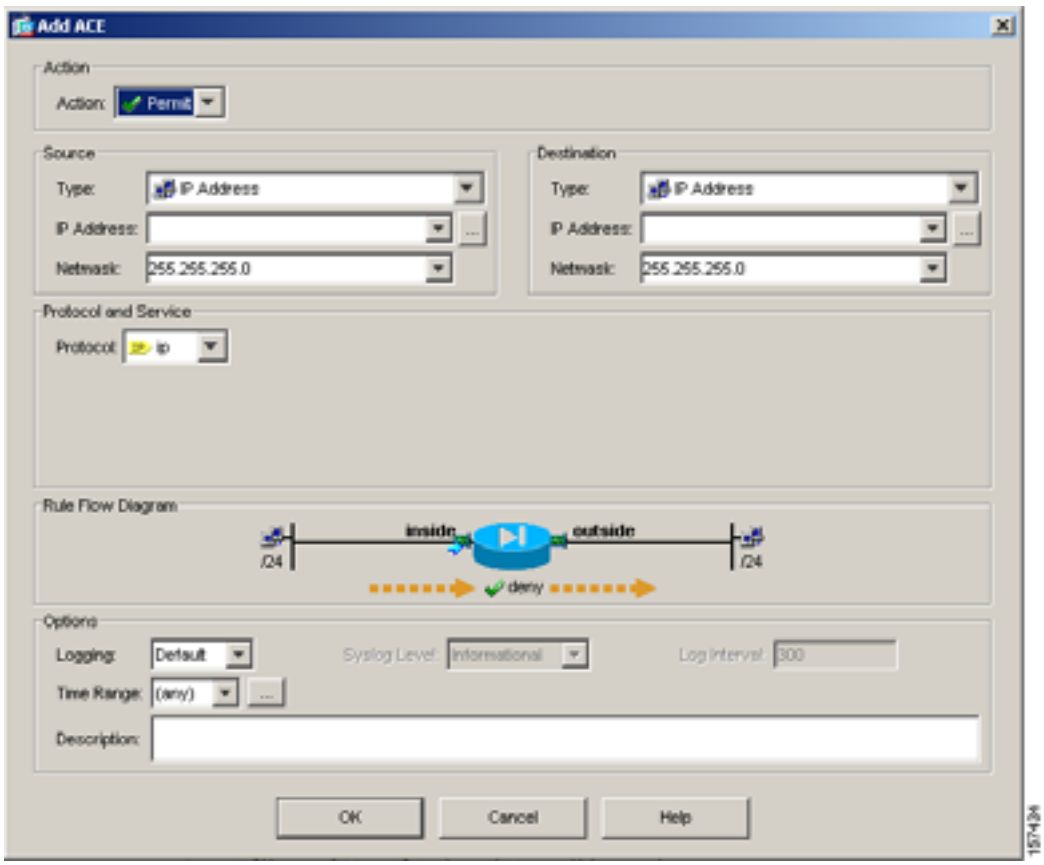
図 2-11　Add ACL ダイアログボックス



ACL を追加した後、**Add ACE** メニューの選択を使用して、フィルタ ルールを読み込むことができます。

フィルタ ルールを追加するには、**Add ACE** をクリックします（図 2-10）。フィルタ ルールを編集するには、変更するルールを選択し、**Edit** をクリックします。Add Extended Access List Rule または Edit Extended Access List Rule ダイアログボックスが表示されます（図 2-12）。Edit Extended Access List Rule ダイアログボックスは、タイトルを除き、Add ACE ダイアログボックスと同じです。

図 2-12　Add ACE



このダイアログボックスを使用して、トラフィックを許可するか拒否するかの設定、発信元および宛先ホストまたはネットワークの指定、このルールを適用するプロトコルおよびサービス（発信元および宛先ポート）の指定、適用する時間範囲の指定または新しい時間範囲の定義、システム オプションの設定、サービス グループの管理ができます。オプションで、このルールの説明を入力することもできます。ここで入力したエントリは、ACL Manager ダイアログボックスの Rule Flow Diagram および Configure ACLs テーブルに表示されます。

（注） このダイアログボックスの Source、Destination、Protocol and Service、Rule Flow Diagram、および Options の各領域の内容は、選択によって変化します。

Source 領域および Destination 領域の設定

これらの領域を使用して、発信元および宛先ネットワークを識別します。発信元および宛先の両方の領域で、次のパラメータを指定します。

- Type：このルールを適用する発信元または宛先アドレスのタイプを選択します。ネットワークは、IP アドレス、インターフェイス IP、またはネットワーク オブジェクト グループで識別できます。キーワード ***any*** を選択して、このルールを任意の発信元または宛先に適用するように指定することもできます。any タイプには、発信元または宛先を表す追加の修飾フィールドはありません。

— IP address および Netmask：Type フィールドで IP Address を選択した場合は、IP address フィールドを使用して発信元または宛先ネットワークまたはホストの IP アドレスを指定し、Netmask フィールドを使用して指定した IP アドレスのサブネット マスクを選択します。たとえば、アドレス / ネットマスクが 192.168.10.0/255.255.255.0 の場合はネットワークが指定され、192.168.10.1/255.255.255.255 の場合はホストが指定されます。デフォルトはありません。

— Browse (...)：（IP アドレスを手動で入力する代わりに）IP アドレスを参照します。Browse をクリックすると、Browse Source（または Destination) Address ダイアログボックス（図 2-13）が開き、すでに設定されているオブジェクトを選択するか、選択したオブジェクト タイプを追加、編集、または削除できます。Browse Source Address ダイアログボックスのツールバーから Add または Edit を選択すると、選択したオブジェクト タイプの Add または Edit 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、エントリの名前、IP アドレス、および（オプションで）説明を入力または変更します。

図 2-13　Browse Source Address ダイアログボックスと Edit IP Name ダイアログボックス

— Group Name：Type フィールドで Network Object Group を選択した場合、ネットワークおよびホストの名前付きグループ（ネットワーク オブジェクト グループ）を選択、または参照（...）できます。デフォルトはありません。

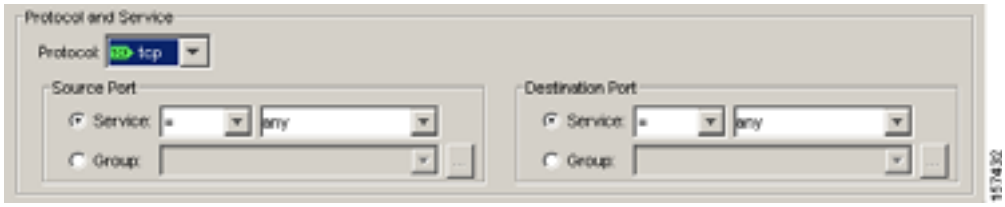
— Interface：Type フィールドで Interface IP を選択した場合、ホストまたはネットワークが常駐するインターフェイスを選択できます。デフォルトは outside です。

プロトコルおよびサービス グループの管理

サービス グループを使用して、ACL と一致させる複数の連続していないポート番号を識別できます。たとえば、ポート番号 5、8、9 で HTTP および FTP をフィルタリングする場合は、これらのすべてのポートを含むサービス グループを定義します。サービス グループを使用しない場合は、ポートごとに個別のルールを作成する必要があります。TCP、UDP、IP、ICMP、およびその他の IP プロトコル用にサービス グループを作成できます。

Add ACE または Edit ACE ダイアログボックスの Protocol and Service 領域で、接続プロトコル、および発信元および宛先ポートのサービス タイプまたはサービス グループを設定します。変更しない場合は、Description フィールドに移動します。図 2-14 に、TCP プロトコルの Protocol and Service 領域を示します。

図 2-14　Protocol and Service 領域（TCP プロトコル）



複数の TCP または UDP サービス（ポート）を 1 つの名前付きグループに関連付けることができます。以後、アクセスや、IPSec ルール、コンジットなどの ASDM および CLI 内の機能でサービス グループを使用できます。

用語の *サービス*は、既知のポート番号と「リテラル」名（ftp、telnet、smtp など）を持つ、アプリケーション レベル サービスと関連付けられた上位レイヤ プロトコルを指します。

セキュリティ アプライアンスは、次の TCP リテラル名を許可します。bgp、chargen、cmd、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、ident、irc、klogin、kshell、lpd、nntp、pop2、pop3、pptp、smtp、sqlnet、sunrpc、tacacs、talk、telnet、time、uucp、whois、www。

サービス グループの**名前**は、オブジェクト グループのすべてのタイプで、一意である必要があります。たとえば、**service** グループと **network** グループで、同じ名前を共有することはできません。

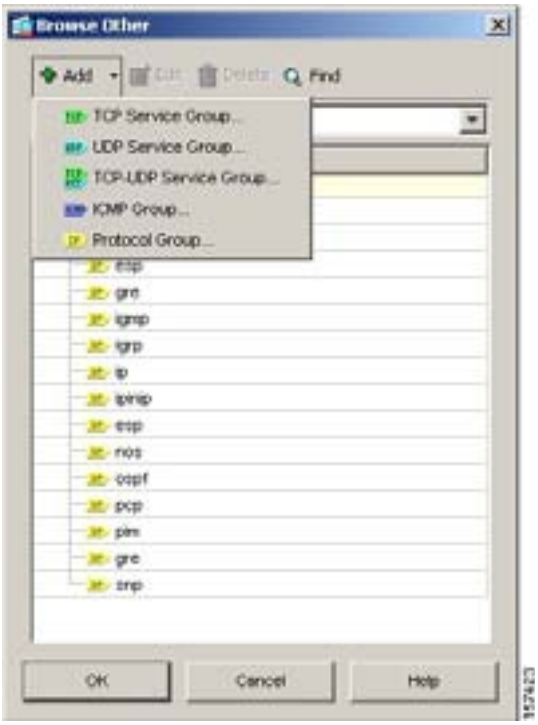
複数のサービス グループを「グループのグループ」にネストして、単一グループとして使用できます。サービス オブジェクト グループを削除すると、使用されているすべてのサービス オブジェクト グループから削除されます。

サービス グループがアクセス ルールで使用されている場合は、削除しないでください。アクセス ルールで使用されているサービス グループを空にすることはできません。

Protocol and Service 領域を使用して、このルールのプロトコルとサービス タイプを指定します。この領域の内容は、プロトコルの選択によって変化します。

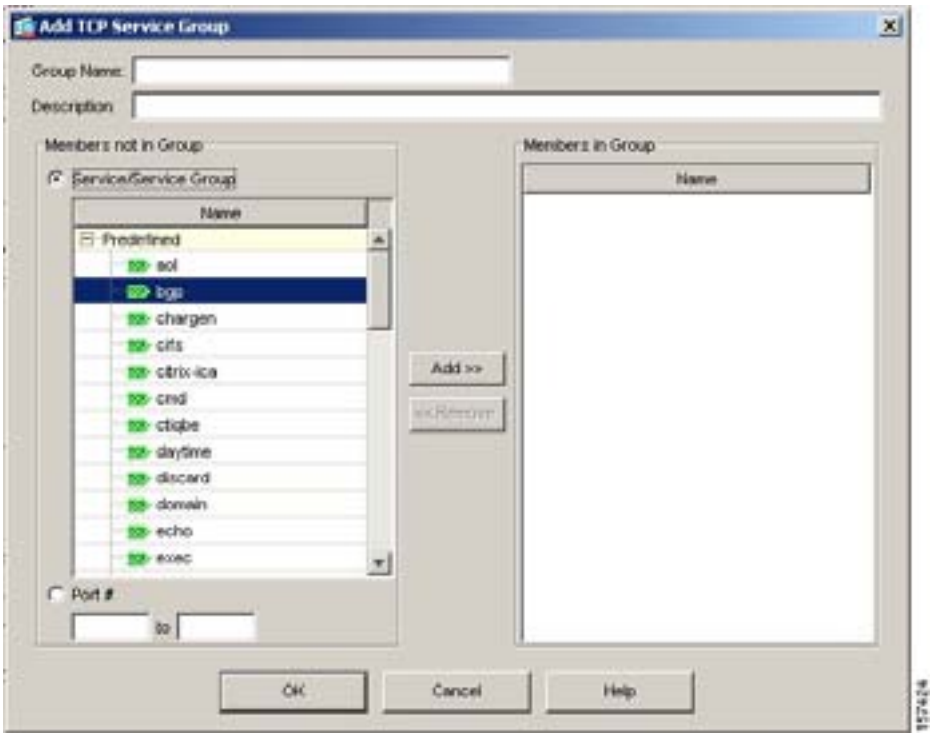
- Protocol：ルールのプロトコルを選択します。使用できる値は、TCP、UDP、ICMP、IP、および IP Other です。この選択によって、この領域の他のフィールドが使用可能になります。
  - IP を選択した場合、追加のフィールドは表示されません。
  - IP Other を選択した場合、Other 領域が表示されます。この領域では、Protocol または Protocol Group を選択できます。Protocol を選択すると、プロトコルを選択できるドロップダウン リストが有効になります。Protocol Group を選択すると、プロトコル グループを選択できるドロップダウン リストが有効になります。または、Browse (...) をクリックして、Browse Other ダイアログボックス（図 2-15）を開くこともできます。このダイアログボックスには事前定義済みの IP プロトコルの名前がリストされ、選択するか、新しいプロトコル サービス グループを作成できます。

図 2-15　Browse Other ダイアログボックス



Add メニューでサービス グループのいずれかを選択すると、選択したプロトコルの Add Service Group ダイアログボックスが開きます。図 2-16 に、その他すべての Add Service Group ダイアログボックスの代表として、Add TCP Service Group ダイアログボックスを示します。

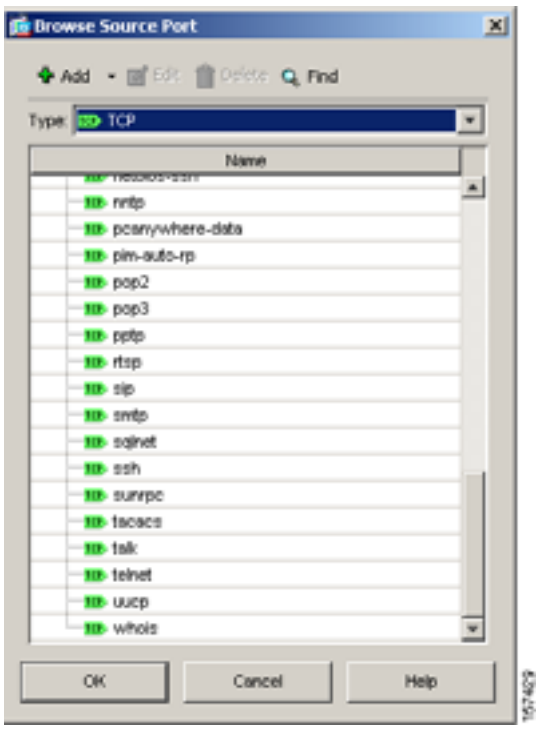
図 2-16　Add TCP Service Group ダイアログボックス



このダイアログボックスで、グループ名および説明の指定、サービスまたはサービス グループの選択またはポートまたはポート範囲の選択、およびグループのメンバへの追加またはメンバからの削除ができます。

- Source/Destination Port：（TCP および UDP）Type で TCP または UDP を選択した場合、Source Port 領域と Destination Port 領域が表示されます。これらの領域のフィールドを使用して、ACL がパケットを照合するために使用するポート番号、ポート範囲、またはサービスのリストにある既知のサービス名（HTTP、FTP など）を指定します。
- Service：（TCP および UDP）演算子リストで、ACL がポートを照合する方法を指定します。次のいずれかの演算子を選択します。=（ポート番号と等しい）、not =（ポート番号と等しくない）、>（ポート番号より大きい）、<（ポート番号より小さい）、range（範囲内のポート番号のいずれかと等しい）。
- Group：（TCP および UDP）サービス グループをドロップダウン リストから選択するか、Browse (...) をクリックして、発信元または宛先ポートの選択、追加、編集、削除、または発信元または宛先ポート グループの作成ができる Browse Source（または Destination）Port ダイアログボックス（図 2-17）を開きます。

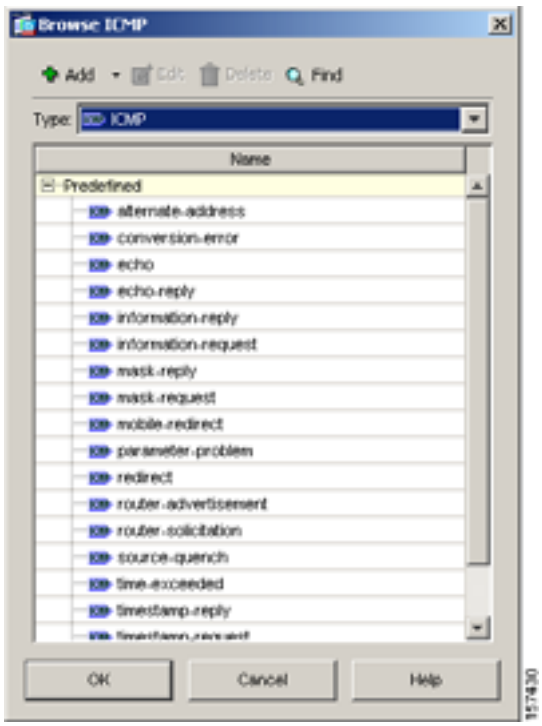
図 2-17　Browse Source Port



Add メニューでサービス グループのいずれかを選択すると、選択したプロトコルの Add Service Group ダイアログボックスが開きます。図 2-16 に、その他すべてのダイアログボックスの代表として、Add TCP Service Group ダイアログボックスを示します。

- Type で ICMP を指定した場合、ICMP 領域が表示されます。ICMP Type を選択し、ドロップダウン リストまたは ICMP Group から選択できます。ICMP Group を選択した場合は、ドロップダウン リストから選択するか、Browse をクリックして Browse ICMP ダイアログボックス（図 2-18）を開き、事前定義済みのリストから ICMP グループを選択できます。

図 2-18　Browse ICMP ダイアログボックス

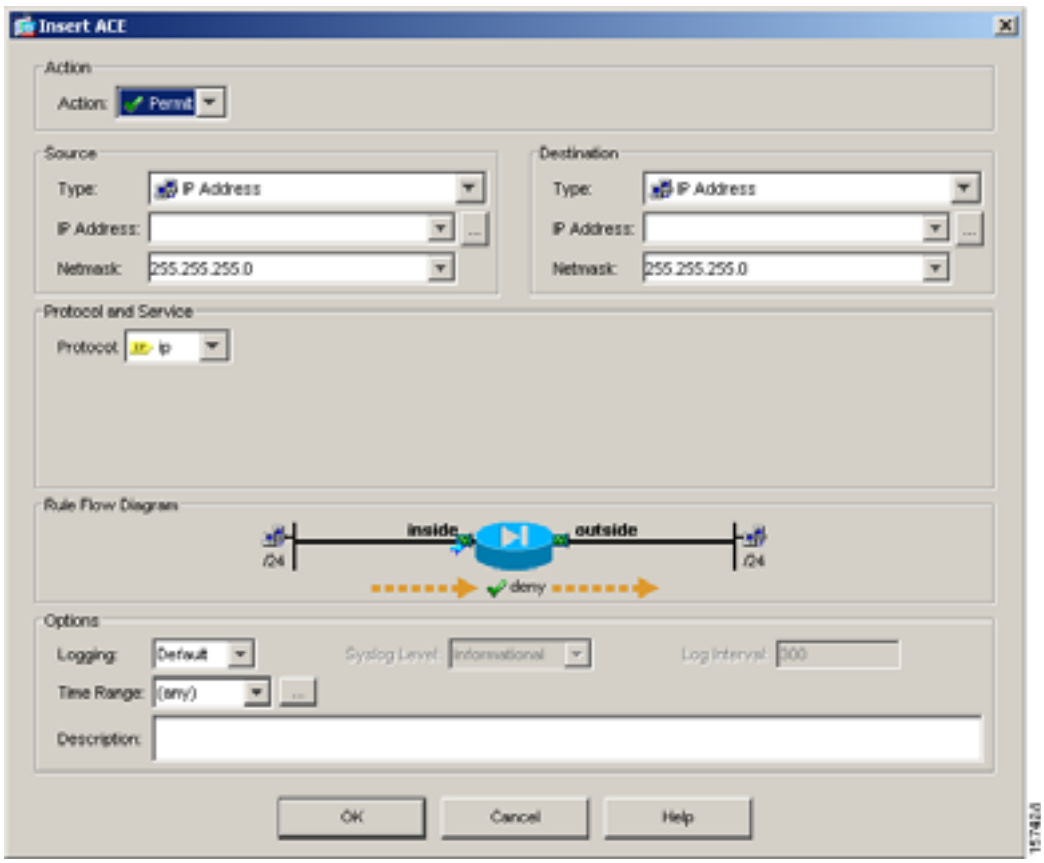


Add メニューでサービス グループのいずれかを選択すると、選択したプロトコルの Add Service Group ダイアログボックスが開きます。図 2-16 に、その他すべてのダイアログボックスの代表として、Add TCP Service Group ダイアログボックスを示します。

ACL ルールの挿入

ACE ルールは、ACL Manager テーブルに現れる順に評価されます。ACL Manager テーブルの特定の位置にルールを挿入するには、まず、既存の ACE を選択し、Add メニューから Insert または Insert After を選択します。選択すると、それぞれ Insert ACE および Insert After ACE ダイアログボックス（図 2-19）が開き、作成する ACE のアトリビュートを指定できます。これら 2 つのダイアログボックスは、タイトルを除き、同じです。Insert は、選択された ACE の上に新しい ACE を挿入し、Insert After は、選択された ACE の下に新しい ACE を挿入します。

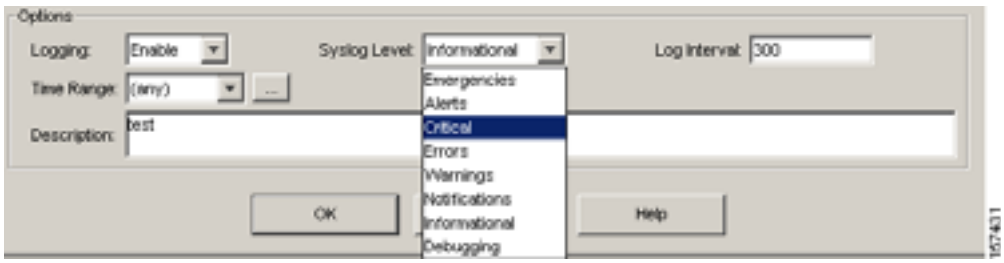
図 2-19　Insert ACE ダイアログボックス



オプションの設定

Options ダイアログボックスを使用して、各 ACE ルールのオプションを設定できます。Options 領域のフィールド（図 2-20）は、ロギング パラメータ、時間範囲、説明など、このルールのオプション機能を設定します。これらのオプションを設定するときは、次のフィールドの説明を参照してください。

図 2-20　Options 領域（Add または Edit ACE ダイアログボックス）



- Logging：ロギングを有効または無効にします。または、デフォルト ロギング設定を使用するように指定します。ロギングを有効にすると、Syslog Level および Log Interval フィールドが使用可能になります。

  ロギングを有効にすると、セキュリティ アプライアンスは、ルールによって新しいフローが許可または拒否されたときに syslog メッセージを生成します。後続の syslog メッセージは、ログ間隔の終了時に生成され、フローのヒット カウントが要約されます。デフォルトの間隔は 300 秒です。
- Syslog Level：ロギング アクティビティのレベルを選択します。デフォルトは Informational です。
- Log Interval：許可および拒否のロギング間隔を指定します。セキュリティ アプライアンスがフロー統計情報を syslog に送信するまで待機する時間です。この設定は、ACE と一致するパケットがない場合にフローを削除するタイムアウト値としても機能します。デフォルトは 300 秒です。範囲は 1 ～ 600 秒です。

（注） コンジット リストおよびアウトバウンド リストはロギングをサポートしません。グローバル ロギング オプションの設定方法については、Configuration > Properties > Logging > Logging Setup に続くウィンドウのオンライン ヘルプを参照してください。

デフォルトのロギング動作は、パケットが拒否された場合にセキュリティ アプライアンスがログ メッセージ 106023 を生成します。パケットが許可された場合は、syslog メッセージは表示されません。デフォルトのロギング動作に戻すには、このオプションを選択します。

デフォルトでは、syslog メッセージは情報レベル（レベル 6）で生成されます。Syslog Level フィールドのドロップダウン リストから選択して、別のレベルのロギング メッセージを syslog サーバに送信するように選択できます。ログレベルは次のとおりです。

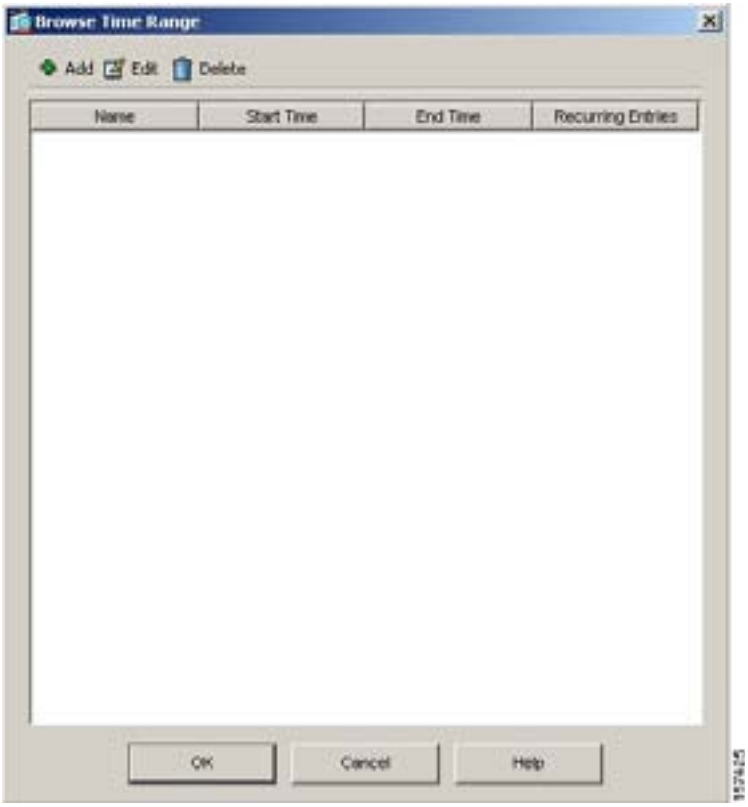
- Emergencies（レベル 0）：セキュリティ アプライアンスでは、このレベルは使用しません。
- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Errors（レベル 3、エラー条件）
- Warnings（レベル 4、警告条件）
- Notifications（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ中のみ表示）

パケットが ACE と一致した場合、セキュリティ アプライアンスはフロー エントリを作成して、指定された間隔で受信したパケットの数を追跡します（Logging Interval フィールドの説明を参照）。セキュリティ アプライアンスは、各間隔の最初のヒット時と終了時に syslog メッセージを作成し、その間隔での合計ヒット数を識別します。各間隔の終了時に、セキュリティ アプライアンスはヒット カウントを 0 にリセットします。その間隔でパケットが ACE と一致しなかった場合、セキュリティ アプライアンスはフロー エントリを削除します。

（注） ロギングを有効にすると、一定量のメモリを消費します。

- Time Range：このルールを使用する時間範囲の名前を選択します。デフォルトは (any) です。Browse (...) ボタンをクリックして Browse Time Range ダイアログボックスを開き、時間範囲を選択または追加します（図 2-21）。

図 2-21　Browse Time Range



時間範囲は、このグループ ポリシーを使用してユーザがセキュリティ アプライアンスに接続できるアクセス時間の範囲を指定します。ACL 設定機能から時間範囲を追加または編集するには、Browse Time Range ツールバーの Add または Edit をクリックします。Add Time Range または Edit Time Range が表示されます。図 2-22 に、Add Time Range ダイアログボックスを示します。

- Description：（オプション）このルールの簡単な説明を示します。説明行の長さは最大 100 文字ですが、説明を改行して複数行にすることができます。

全般的な VPN 接続設定アトリビュートの設定

この項の手順に従って、VPN 接続アトリビュートの値を設定するアトリビュートを設定します。これらのアトリビュートは、許可される同時ログイン数、VPN 接続に使用する ACL 名、およびトンネル プロトコルを制御します。この項のすべてのアトリビュートで、Inherit チェックボックスを選択することによって、デフォルト グループ ポリシーからグループ ポリシーに値を継承することができます。

アクセス時間の設定

VPN アクセス時間は、このグループのユーザがセキュリティ アプライアンスに接続できる時間を決定します。VPN アクセス時間を設定するには、すでに設定している時間範囲ポリシーにグループ ポリシーを関連付けます。時間範囲ポリシーは、実際のアクセス時間を決定します。

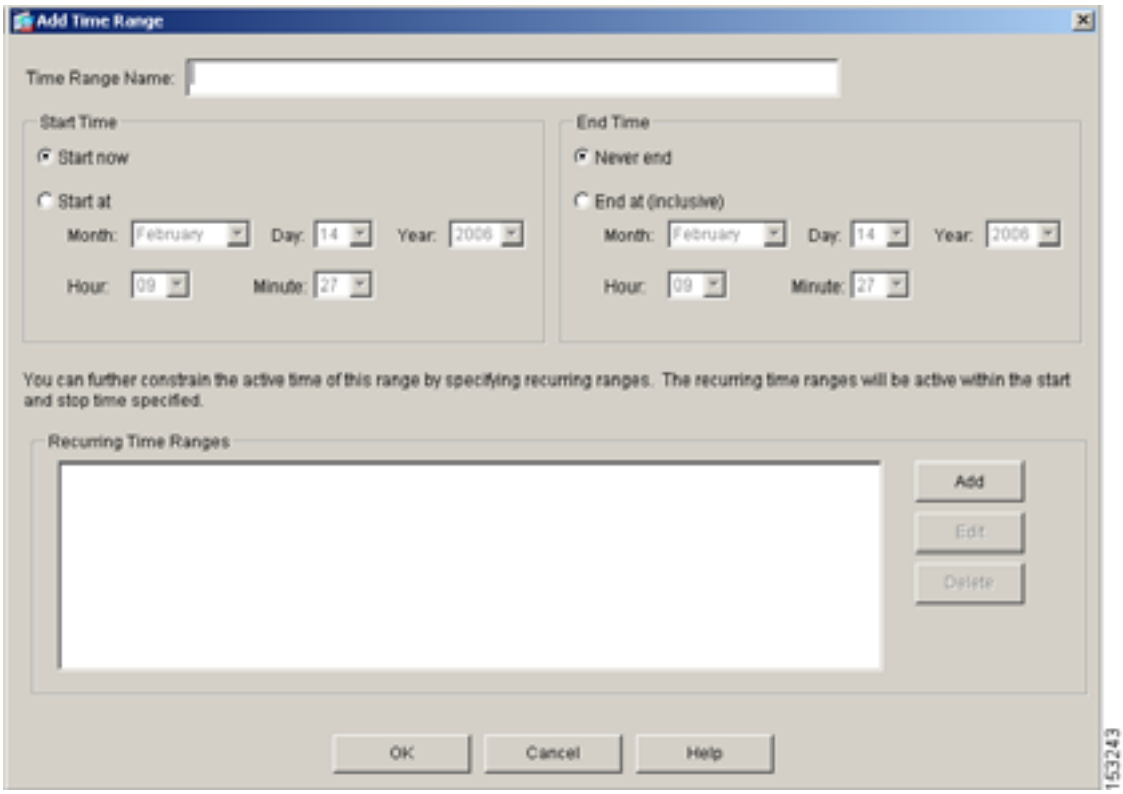
時間範囲は、このグループ ポリシーを使用してユーザがセキュリティ アプライアンスに接続できるアクセス時間の範囲を指定する変数です。アクセス時間を制限するには、メニューから時間範囲の名前を選択します。

既存の時間範囲の特性を表示するには、Configuration > Global Objects > Time Ranges を選択します。既存の時間範囲を選択して ACL フィルタで使用するには、Add/Edit ACE ダイアログボックスの Time Range ドロップダウン メニューから名前を選択します。このフィルタで時間範囲を制限しない場合は、メニューから **Unrestricted** を選択します。どちらの場合でも、新しい時間範囲を定義しない場合は、P.2-27 の「同時ログインの設定」までスキップします。

Inherit チェックボックスを選択すると、グループ ポリシーからアクセス時間変数をグループ ポリシーに継承できます。このオプションを選択する場合は、P.2-27 の「同時ログインの設定」までスキップします。

General タブから時間範囲を追加または編集するには、Inherit チェックボックスをクリアし、Manage をクリックします。Browse Time Range ダイアログボックスが表示されます。または、Add ACE または Edit ACE ダイアログボックスの Time Range 領域で Browse (...) をクリックして、Browse Time Range ダイアログボックスを開きます。Add Time Range または Edit Time Range ダイアログボックスが表示されます（図 2-22）。既存の時間範囲を編集する場合、Time Range Name フィールドは表示専用です。

図 2-22　Add Time Range ダイアログボックス

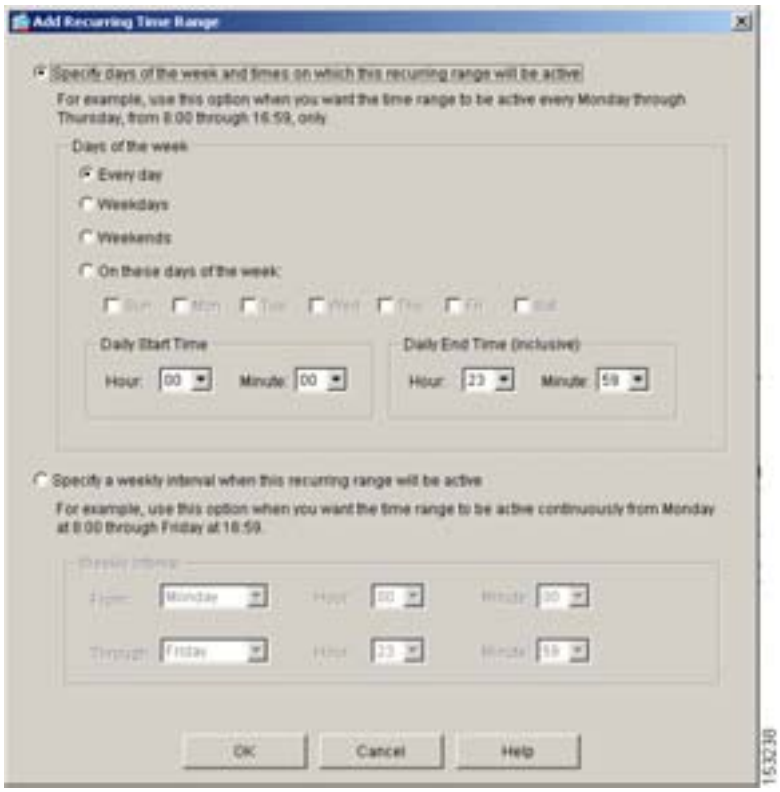


時間範囲を追加する場合は、この時間範囲の名前を指定できます。必要な場合、時間範囲を使用するグループ ポリシーを設定するときに、ドロップダウン リストからこの名前を選択して、この時間範囲を選択できます。

開始時間と終了時間を指定します。開始時間と終了時間を設定するときは、両端の時間が含まれることに注意してください。

指定された開始時間と終了時間の間でアクティブになる繰り返し時間範囲を指定することで、時間範囲のアクティブ時間をさらに制約できます。繰り返し時間範囲を削除するには、範囲を選択し、**Delete** をクリックします。繰り返し時間範囲を追加するには、**Add** をクリックするか、既存の時間範囲を選択して **Edit** をクリックします。Add Recurring Time Ranges または Edit Recurring Time Ranges ダイアログボックスが表示されます（図 2-23）。

図 2-23　Add Recurring Time Ranges または Edit Recurring Time Ranges ダイアログボックス



繰り返し範囲をアクティブにする曜日と時間、または繰り返し範囲をアクティブにする毎週の間隔として繰り返し時間範囲を指定し、OK をクリックします。OK をクリックして、Add Time Range ダイアログボックスでの設定を完了します。

同時ログインの設定

任意のユーザに対して、許可される同時ログイン数を指定できます。デフォルト値は 3 です。範囲は 0 ～ 2147483647 の整数です。グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。0 を入力すると、ログインが無効になり、ユーザがアクセスできなくなります。

注意　同時ログイン数の上限は非常に大きいですが、この値を設定するとセキュリティ上の危険が発生し、パフォーマンスに影響を与えることがあります。

最大接続時間の設定

VPN 接続の最大時間を設定します。この時間の終了時に、セキュリティ アプライアンスは接続を終了します。接続時間を無制限にするには、Unlimited チェックボックスを選択します。特定の時間制限を設定するには、Unlimited チェックボックスをクリアします。これによって、minutes フィールドが使用可能になります。最小時間は 1 分で、最大時間は 35791394 分です。デフォルト値はありません。

ユーザ アイドル タイムアウトの設定

Unlimited チェックボックスを選択するか、システムをアイドル状態のままにできる時間を分単位で指定して、ユーザ アイドル タイムアウト時間を設定します。この時間、接続で通信アクティビティがなかった場合、セキュリティ アプライアンスは接続を終了します。最小時間は 1 分で、最大時間は 35791394 分です。デフォルトは 30 分です。

WINS サーバ、DNS サーバ、および DHCP スコープの設定

プライマリおよびセカンダリ WINS サーバおよび DNS サーバ、および DHCP スコープを設定できます。それぞれのデフォルト値はありません。これらのアトリビュートを設定するには、次の手順を実行します。

ステップ 1　プライマリおよびセカンダリ DNS サーバを指定します。指定する最初の IP アドレスは、プライマリ DNS サーバの IP アドレスです。2 番目の（オプションの）IP アドレスは、セカンダリ DNS サーバの IP アドレスです。最初のフィールドで IP アドレスを指定せずにブランクのままにすると、DNS サーバがヌル値に設定されます。この場合、DNS サーバが指定されず、デフォルトまたは特定のグループ ポリシーから値を継承しません。

DNS サーバの値を入力するたびに、既存の設定が上書きされます。たとえば、10.10.10.15 としてプライマリ DNS サーバを設定した後、プライマリ DNS サーバを 10.10.10.30 に設定した場合、後の指定で最初の指定が上書きされ、10.10.10.30 がプライマリ DNS サーバになります。

ステップ 2　プライマリおよびセカンダリ WINS サーバを指定します。指定する最初の IP アドレスは、プライマリ WINS サーバの IP アドレスです。2 番目の（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。IP アドレスの代わりに ***none*** キーワードを指定すると、WINS サーバがヌル値に設定されます。この場合、WINS サーバが指定されず、デフォルトまたは特定のグループ ポリシーから値を継承しません。

wins-server コマンドを入力するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定した後、WINS サーバ y.y.y.y を設定すると、2 番目のコマンドで最初のコマンドが上書きされ、y.y.y.y だけが WINS サーバになります。複数のサーバの場合も同じです。前に設定したサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときに、すべての WINS サーバの IP アドレスを含めます。

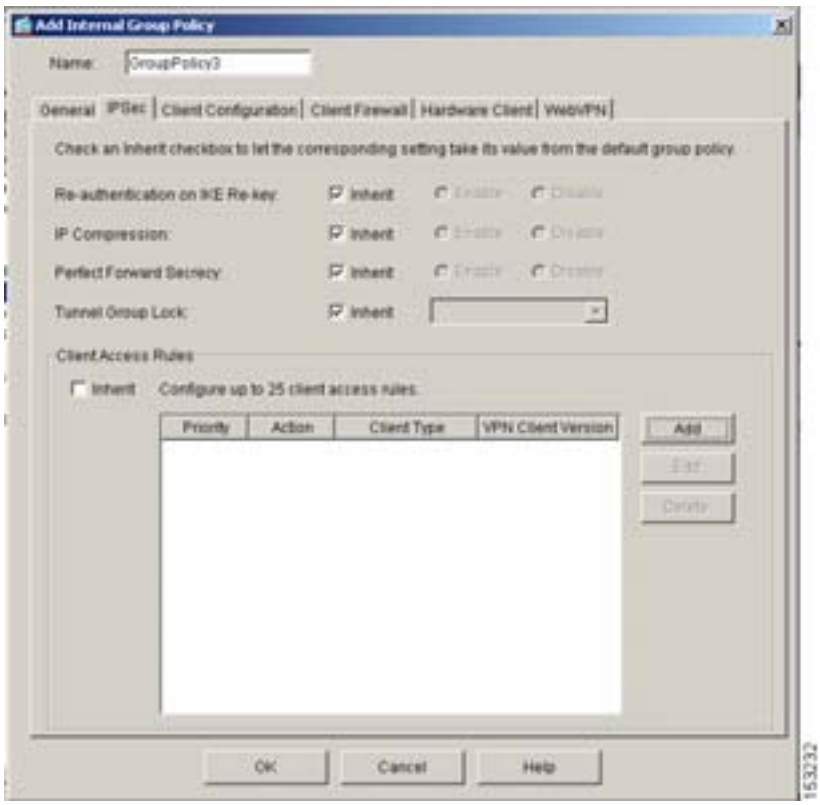
次の例で、FirstGroup というグループ ポリシーに IP アドレス 10.10.10.15 と 10.10.10.30 の WINS サーバを設定する方法を示します。

ステップ 3　DHCP スコープを指定します。これは、このグループ ポリシーのユーザにアドレスを割り当てるときにセキュリティ アプライアンス DHCP サーバが使用するサーバ IP アドレスの範囲です。たとえば、グループ ポリシーに IP サブネットワーク 10.10.85.0（10.10.85.0 ～ 10.10.85.255 のアドレス範囲を指定）を設定するには、DHCP スコープを 10.10.85.0 に指定する必要があります。

IPSec アトリビュートの設定

Add Internal Group Policy または Edit Internal Group Policy ウィンドウの IPSec タブを使用して、このグループ ポリシーのセキュリティ アトリビュートを指定できます。図 2-24 に、IPSec タブを示します。

図 2-24　Add Internal Group Policy ウィンドウの IPSec タブ



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。次の項で、このタブのアトリビュートの設定方法について説明します。

IKE 鍵の再生成での再認証の設定

Enable または Disable を選択して、IKE 鍵の再生成でユーザの再認証を必要とするかどうかを指定します。IKE 鍵の再生成での再認証を有効にした場合、セキュリティ アプライアンスは、最初の Phase 1 IKE ネゴシエーションの際にユーザ名とパスワードを入力するようにユーザに要求し、さらに、IKE 鍵の再生成が発生するたびにユーザの再認証を要求します。再認証を行うと、セキュリティが強固になります。Inherit チェックボックスをクリアした場合、IKE 鍵の再生成での再認証はデフォルトで無効になります。

設定された鍵の再生成の間隔が非常に短い場合、認証の要求が繰り返されることをユーザが不便に感じることがあります。認証の要求が繰り返されないようにするには、再認証を無効にします。設定されている鍵の再生成の統計情報をチェックするには、**Monitoring > VPN > VPN Statistics > Crypto Statistics** を選択して、セキュリティ アソシエーション統計情報を表示します。

（注）　接続の他方にユーザがいない場合、再認証は失敗します。

IP 圧縮の設定

IP 圧縮を有効にするかどうかを指定します。デフォルトでは無効になっています。データ圧縮を有効にすると、モデムで接続しているリモート ダイヤルイン ユーザに対するデータ転送速度が速くなります。デフォルトでは、IP 圧縮は無効になっています。

注意　データ圧縮を行うと、ユーザ セッションごとのメモリ要件および CPU 使用率が高くなり、その結果、セキュリティ アプライアンスの全体的なスループットが低下します。そのため、モデムで接続しているリモート ユーザに対してのみ、データ圧縮を有効にすることをお勧めします。モデム ユーザに固有のグループ ポリシーを設計し、これらのユーザに対してのみ圧縮を有効にします。

LZS IP 圧縮を有効または無効にするには、**Enable** または **Disable** を選択します。

完全転送秘密の設定

perfect forward secrecy（PFS; 完全転送秘密）を有効にするかどうかを指定します。IPSec ネゴシエーションで完全転送秘密を使用すると、新しい各暗号鍵が前の鍵と無関係になることが保証されます。Inherit チェックボックスを選択すると、デフォルト グループ ポリシーから完全転送秘密の値をグループ ポリシーに継承できます。選択しない場合、デフォルトで、完全転送秘密は無効になります。完全転送秘密を有効または無効にするには、**Enable** または **Disable** を選択します。

トンネル グループ ロックの設定

Tunnel Group Lock アトリビュートを有効または無効にして、リモート ユーザが必ずトンネル グループを経由してアクセスするように制限するかどうかを指定します。

Add Internal Group Policy または Edit Internal Group Policy の IPSec タブで、Inherit チェックボックスを選択解除し、ドロップダウン リストからトンネルグループ名を選択します。このグループ ポリシーに関連付けられているユーザは、指定されたトンネル グループを経由した場合にのみアクセスできるようになります。

トンネルグループ名は、ユーザが接続するためにセキュリティ アプライアンスで要求される既存のトンネル グループの名前を指定します。トンネル グループ ロックは、VPN クライアントで設定されているグループが、ユーザが割り当てられているトンネル グループと同じかどうかをチェックすることで、ユーザを制約します。同じでない場合、セキュリティ アプライアンスは、ユーザが接続できないようにします。トンネル グループ ロックを設定しない場合、セキュリティ アプライアンスは、割り当てられているグループを考慮せずにユーザを認証します。デフォルトでは、グループ ロックは無効になっています。

グループ ポリシー設定からグループ ロックを削除するには、リストから None を選択します。このオプションは、グループ ロックをヌル値に設定するため、グループ ロック制限をなしにできます。また、デフォルト グループ ポリシーまたは特定のグループ ポリシーからのグループ ロック値の継承も抑止します。

クライアント アクセス ルールの設定

Client Access Rules 領域を使用して、VPN クライアントの特定のタイプおよびバージョンごとに、アクセスを許可または拒否する 25 までのルールを指定できます。グループ ポリシーは、これらのルールをデフォルト グループ ポリシーから継承することも、このグループ ポリシーに固有のルールを指定することもできます。

この領域のテーブルには、各ルールで指定された優先順位、アクション、クライアント タイプ、および VPN クライアント バージョンが表示されます。

セキュリティ アプライアンスを介して IPSec 経由で接続できるリモート アクセス クライアントのタイプおよびバージョンを制限するルールを設定するには、**Inherit** チェックボックスをクリアします。これによって、テーブルに関連付けられているボタンがアクティブになります。デフォルトでは、アクセス ルールはありません。クライアント アクセス ルールがない場合、すべてのクライアント タイプおよびバージョンがアクセスできます。個別のルールを削除するには、**Delete** をクリックします。

Client Access Rules テーブルのカラムは、次のとおりです。

- Priority：このルールの優先順位が表示されます。ルールの優先順位を決定します。最も小さな整数のルールが、最も高い優先順位です。つまり、クライアント タイプやバージョンと一致した最も小さな整数のルールが適用されます。より低い優先順位のルールが相反している場合、セキュリティ アプライアンスはこれを無視します。
- Action：このルールで、特定のタイプおよびバージョンのクライアントのアクセスが許可されるか拒否されるかを指定します。
- 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 クライアントかサブセットかを指定します。自由形式の文字列でデバイスタイプを識別します（VPN 3002 など）。文字列は、show vpn-sessiondb remote display での表示と正確に一致する必要があります。ただし、ワイルドカードとして * 文字を使用できます。
- 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）。このボックスには、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。自由形式の文字列でデバイスを識別します（7.0 など）。文字列は、show vpn-sessiondb remote display での表示と正確に一致する必要があります。ただし、ワイルドカードとして * 文字を使用できます。

IPSec グループ ポリシーの新しいルールを追加するには、**Add** をクリックします。IPSec グループ ポリシーの既存のルールを修正するには、**Edit** をクリックします。Add Client Access Rule または Edit Client Access Rule ダイアログボックスが表示されます（図 2-25）。

図 2-25　Add Client Access Rule ダイアログボックス

次の注意事項に従って、ルールを構築します。

- ルールをまったく定義しなかった場合、セキュリティ アプライアンスはすべての接続タイプを許可します。
- クライアントがどのルールにも一致しなかった場合、セキュリティ アプライアンスは接続を拒否します。つまり、拒否ルールを定義する場合は、1 つ以上の許可ルールも定義する必要があります。定義しなかった場合、セキュリティ アプライアンスはすべての接続を拒否します。

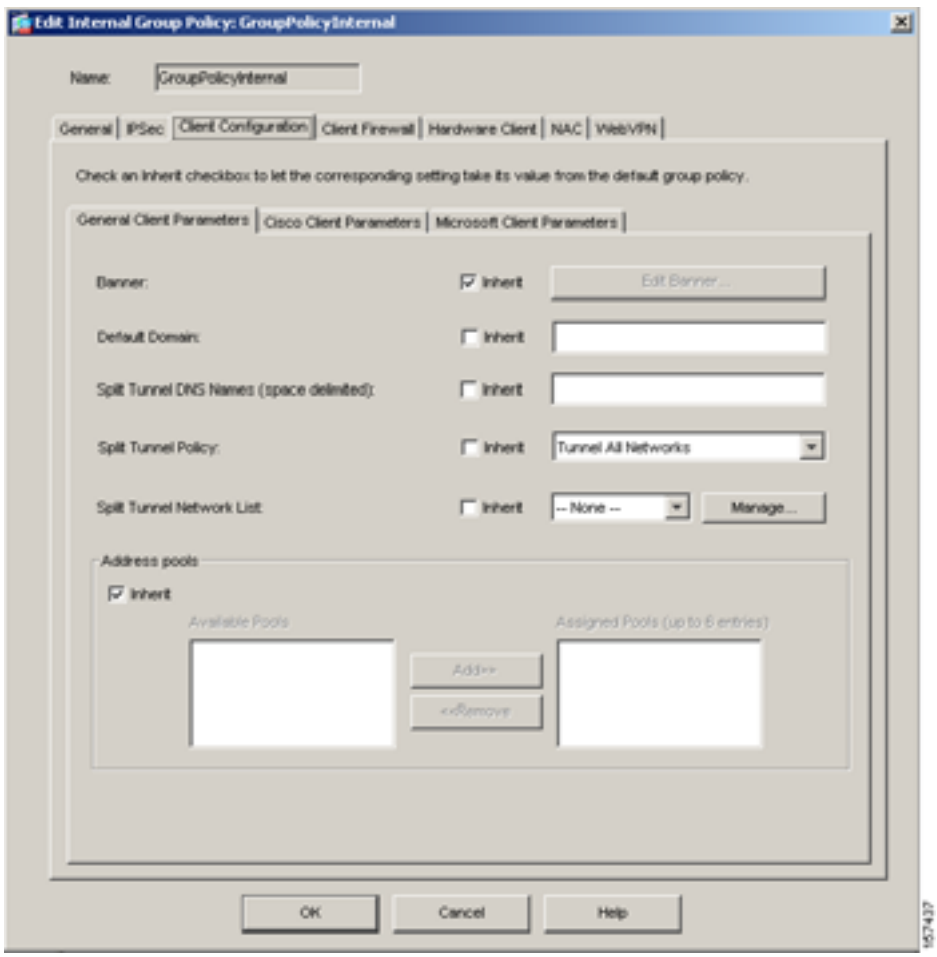
- ソフトウェア クライアントとハードウェア クライアントのどちらも、タイプとバージョンは **Monitoring > VPN > VPN Statistics > Sessions** ウィンドウでの表示と正確に一致する必要があります。
- * 文字はワイルドカードで、各ルールで複数回使用できます。たとえば、クライアント アクセス ルールで VPN クライアント バージョンを **version 3.*** と指定した場合、このルールは、リリース バージョン 3.x のソフトウェアを実行している指定されたクライアント タイプに適用されます。
- 1 つのグループ ポリシーには、最大 25 のルールを構築できます。
- ルール セットの全体で 255 文字という上限があります。
- クライアント タイプまたはバージョンを送信しないクライアントには、n/a を使用できます。

クライアント設定パラメータの設定

Add Internal Group Policy または Edit Internal Group Policy ウィンドウの Client Configuration タブ（図 2-26）は、次のタブで構成されます。

- General Client Parameters
- Cisco Client Parameters
- Microsoft Client Parameters

図 2-26　General Client Parameters タブ

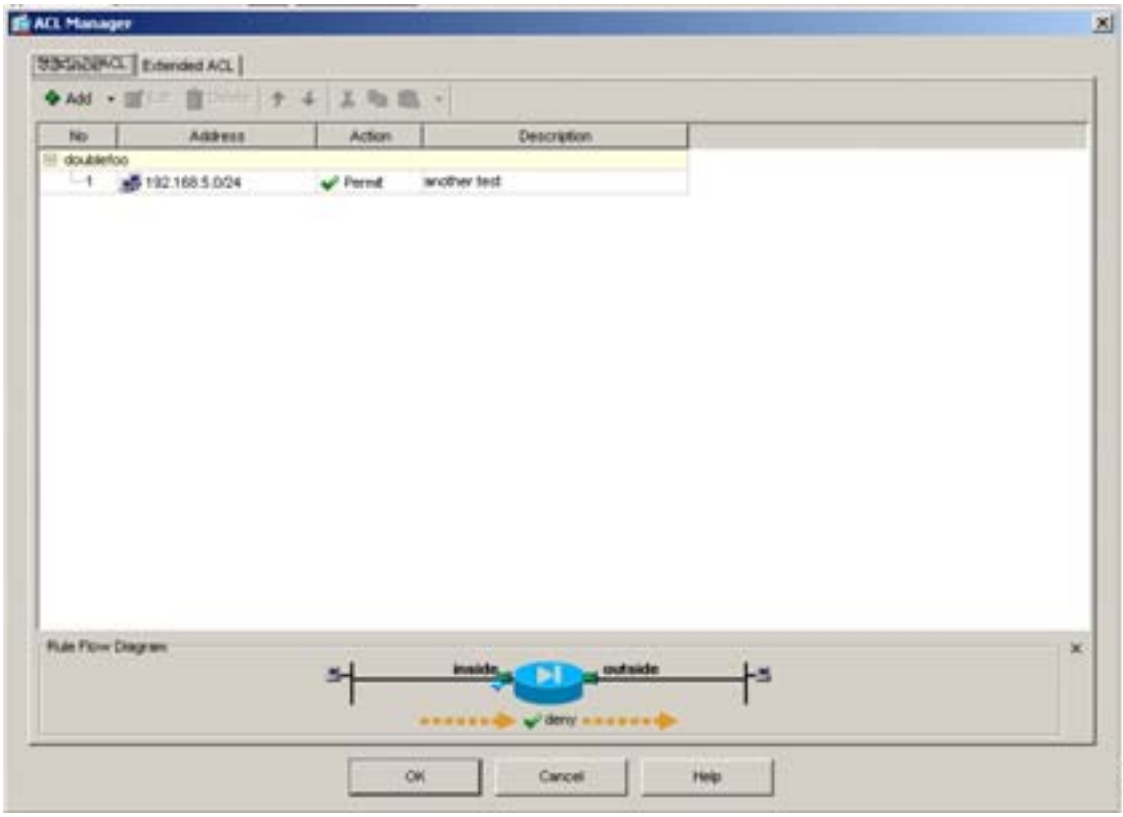


全般的なクライアント パラメータの設定

General Client Parameters タブでは、バナー テキスト、デフォルト ドメイン、スプリット トンネル パラメータ、アドレス プールなど、Cisco クライアントと Microsoft クライアントに共通のクライアント アトリビュートを設定します。ほとんどの場合、Inherit チェックボックス（デフォルトで選択）を使用して、対応する設定の値をデフォルト グループ ポリシーから取得するように指定できます。Inherit チェックボックスをクリアすると、パラメータのその他のオプションが使用できるようになります。全般的なクライアント パラメータを設定するときは、次のフィールドの説明を参照してください。

- Banner：デフォルト グループ ポリシーからバナーを継承するか、新しいバナー テキストを入力するかを指定します。
- Edit Banner：View/Config Banner ダイアログボックスが表示され、500 文字までのバナー テキストを入力できます。詳細については、P.2-35 の「バナー メッセージの設定」を参照してください。
- Default Domain：デフォルト グループ ポリシーからデフォルト ドメインを継承するか、このフィールドで指定する新しいデフォルト ドメインを使用するかを指定します。このフィールドと、次のトンネリング関連フィールドの詳細については、「トンネリング用ドメイン アトリビュートの設定」を参照してください。
- Split Tunnel DNS Names (space delimited)：デフォルト グループ ポリシーからスプリットトンネル DNS 名を継承するか、このフィールドで新しい名前または名前のリストを指定するかを指定します。
- Split Tunnel Policy：デフォルト グループ ポリシーからスプリットトンネル ポリシーを継承するか、メニューからポリシーを選択するかを指定します。メニュー オプションは、すべてのネットワークをトンネリングする、下のネットワーク リストに含まれるネットワークをトンネリングする、または下のネットワーク リストに含まれるネットワークを除外するです。
- Split Tunnel Network List：デフォルト グループ ポリシーからスプリットトンネル ネットワーク リストを継承するか、ドロップダウン リストから選択するかを指定します。
- Manage：ACL Manager ダイアログボックス（図 2-27）を開き、標準および拡張アクセス コントロール リストを管理できます。

図 2-27　ACL Manager ダイアログボックスと標準および拡張 ACL



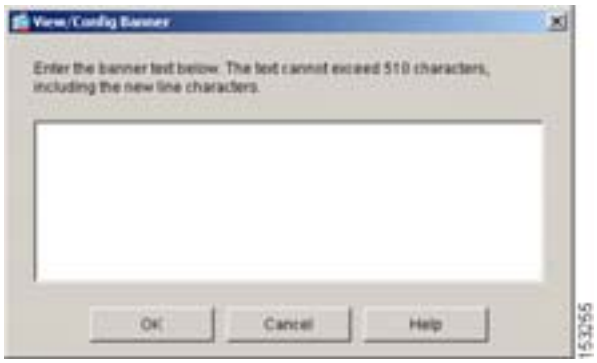
この ACL Manager ダイアログボックスは、「ACL と ACE の管理」で説明したダイアログボックスと機能的には同じですが、標準 ACL と拡張 ACL が 2 つの異なるタブに表示されます。

- Address Pools：このグループ ポリシーを通じて使用できるアドレス プールを設定します。
  - Available Pools：リモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定します。Inherit チェックボックスが選択解除され、Assigned Pools リストにアドレス プールがない場合、アドレス プールは設定されず、グループ ポリシーの他のソースから継承されません。
  - Add：アドレス プールの名前を Available Pools リストから Assigned Pools リストに移動します。
  - Remove：アドレス プールの名前を Assigned Pools リストから Available Pools リストに移動します。
  - Assigned Pools (up to 6 entries)：割り当て済みプール リストに追加したアドレス プールをリストします。このテーブルのアドレス プール設定は、グループのローカル プール設定を上書きします。6 つまでのローカル アドレス プールのリストを指定し、ローカル アドレス割り当てに使用できます。プールを指定する順番には意味があります。セキュリティ アプライアンスは、このコマンドで出現する順序と同じ順序でプールからアドレスを割り当てます。

バナー メッセージの設定

バナーは、リモート クライアントが接続したときに表示されるメッセージです。デフォルトはバナーなしです。デフォルト グループ ポリシーからバナーを継承しない場合は、Inherit チェックボックスをクリアして Edit Banner をクリックします。View/Config Banner ダイアログボックスが表示されます（図 2-28）。

図 2-28　View/Config Banner ダイアログボックス



表示するバナーまたは初期メッセージ（必要な場合）を指定するには、510 文字までの長さのバナーテキストを入力します。「\n」シーケンスを入力すると、復帰記号が挿入されます。

(注)　バナーに含まれる復帰 / 改行は、2 文字としてカウントされます。

バナーを削除するには、テキストを削除します。

トンネリング用ドメイン アトリビュートの設定

トンネリングされたパケット用のデフォルト ドメイン名またはスプリット トンネルで解決されるドメイン リストを指定できます。次の項で、これらのドメインの設定方法について説明します。

トンネリングされたパケット用のデフォルト ドメイン名の定義

セキュリティ アプライアンスは、デフォルト ドメイン名を IPSec クライアントに渡し、ドメイン フィールドが省略されている DNS クエリに追加します。デフォルト ドメイン名がない場合は、ユーザがデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。グループ ポリシーのユーザのデフォルト ドメイン名を指定するには、Inherit チェックボックスをクリアし、フィールドにデフォルト ドメイン名を入力します。

入力したドメイン名は、グループのデフォルト ドメイン名を識別します。デフォルト ドメイン名なしを指定するには、このフィールドをブランクのままにします。このコマンドは、ドメイン名にヌル値を設定し、デフォルト ドメイン名を拒否し、デフォルト グループ ポリシーまたは特定のグループ ポリシーからのデフォルト ドメイン名の継承を抑止します。

スプリット トンネリング用のドメイン リストの定義

スプリット トンネリング用のドメイン リストを指定するには、Inherit チェックボックスをクリアし、スプリット トンネルで解決されるドメインを空白で区切って入力します。スプリット トンネリング ドメイン リストがない場合、ユーザは、デフォルト グループ ポリシーのリストを継承できます。ユーザがスプリット トンネリング ドメイン リストを継承しないようにするには、このリストをブランクのままにします。

ドメイン名アトリビュートは、セキュリティ アプライアンスがスプリット トンネルで解決するドメイン名を指定します。このリストをブランクのままにすると、スプリット DNS リストがないことを示します。また、スプリット DNS リストがヌル値に設定され、その結果、スプリット DNS リストが拒否され、デフォルト グループ ポリシーまたは特定のグループ ポリシーからのスプリット DNS リストの継承が抑止されます。

ドメイン リストの各エントリは、単一の空白で区切ります。エントリ数の制限はありませんが、文字列全体の長さは 255 文字以下にする必要があります。使用できる文字は、英数字、ハイフン（-）、ピリオド（.）だけです。トンネルでデフォルト ドメイン名を解決する場合は、その名前をリストに明示的に含める必要があります。

スプリット トンネリング アトリビュートの設定

スプリット トンネリングを使用すると、リモートアクセス IPSec クライアントが、条件に従ってパケットを暗号化された形式の IPSec トンネルまたはクリア テキスト形式のネットワーク インターフェイスに転送できるようになります。スプリット トンネリングを有効にすると、IPSec トンネルの他方に向けて送信された以外のパケットは、暗号化してトンネルで送信し、暗号化解除して最終的な宛先に経路選択する必要がなくなります。このコマンドは、このスプリット トンネリング ポリシーを特定のネットワークに適用します。

スプリット トンネリング ポリシーの設定

スプリット トンネリング ポリシーを指定して、トラフィックをトンネリングするルールを設定します。デフォルトは、すべてのトラフィックをトンネリングするです。スプリット トンネリング ポリシーを設定するには、Inherit チェックボックスをクリアし、スプリットトンネル ポリシーをドロップダウン メニューから選択します。実行コンフィギュレーションからスプリットトンネル ポリシー アトリビュートを削除するには、このフィールドをブランクのままにします。これによって、別のグループ ポリシーからのスプリット トンネリングの値の継承が有効になります。

- Tunnel All Networks を選択すると、すべてのトラフィックが暗号化され、セキュリティ アプライアンス以外の宛先に送信されないように指定されます。結果として、スプリット トンネリングが無効になります。リモート ユーザは、企業ネットワークを通じてインターネット ネットワークに到達し、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。
- Tunnel Network List Below を選択すると、指定されたネットワークから発信または指定されたネットワークに送信されるすべてのトラフィックがトンネリングされます。このオプションによって、スプリット トンネリングが有効になります。トンネリングするネットワーク アドレスのリストを作成できます。その他すべてのアドレスへのデータは平文で転送され、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ト指定されます。
- Exclude Network List Below を選択して、平文で転送されるネットワークのリストを定義します。この機能は、プリンタなどローカル ネットワークのデバイスにはアクセスせず、トンネルを介して企業ネットワークに接続するリモート ユーザにとって便利です。このオプションは、Cisco VPN クライアントにのみ適用されます。

（注）　スプリット トンネリングは、本来トラフィック管理機能で、セキュリティ機能ではありません。セキュリティを最適化するには、スプリット トンネリングを有効にしないことをお勧めします。

スプリットトンネリング用ネットワーク リストの作成

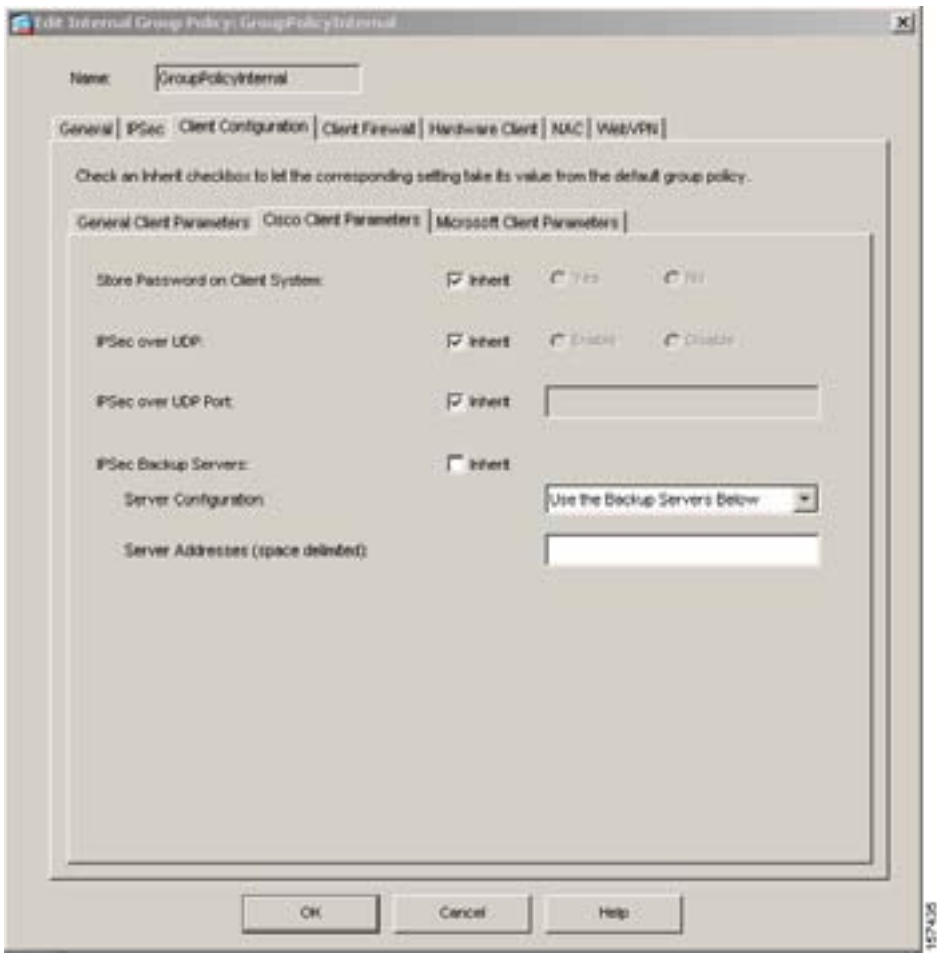
Split Tunnel Network List ドロップダウン メニューから、スプリット トンネリング用のネットワーク リスト名を選択します。スプリット トンネリング ネットワーク リストは、トラフィックがトンネルを経由する必要があるネットワークと、トンネリングを必要としないネットワークを区別します。セキュリティ アプライアンスは、ネットワーク リストに基づいてスプリット トンネリングを決定します。このネットワーク リストは、プライベート ネットワークのアドレス リストで構成された ACL です。標準タイプの ACL だけを使用できます。**Manage** をクリックすると、ACL Manager ダイアログボックスが開き、ACL を設定できます。ACL Manager ダイアログボックスの使用の詳細については、P.2-13 の「ACL フィルタの設定」を参照してください。

選択したアクセスリスト名によって、トンネリングするネットワークまたはトンネリングしないネットワークを列挙したアクセスリストが識別されます。***None*** を選択すると、スプリット トンネリング用のネットワーク リストがなく、セキュリティ アプライアンスがすべてのトラフィックをトンネリングすることを示します。***None*** を選択すると、スプリット トンネリング ネットワーク リストにヌル値が設定され、スプリット トンネリングが拒否されます。また、デフォルト グループ ポリシーまたは特定のグループ ポリシーからのデフォルト スプリット トンネリング ネットワーク リストの継承が抑止されます。

Cisco クライアント パラメータの設定

Cisco Client Parameters タブ（図 2-29）のアトリビュートは、パスワード保管、IPSec over UPD 設定、IPSec バックアップ サーバなど、グループの特定のセキュリティ設定を指定します。

図 2-29　Cisco Client Parameters タブ



パスワード保管の設定

ユーザがログイン パスワードをクライアント システムに保管できるかどうかを指定できます。セキュリティ上の理由により、パスワード保管はデフォルトで無効になっています。パスワード保管は、セキュアなサイトにあることがわかっているシステムでのみ有効にします。

パスワード保管を有効または無効にするには、Store Password on Client System アトリビュートの Inherit チェックボックスをクリアし、**Yes**（有効）または **No**（無効）を選択します。

このアクションは、インタラクティブ ハードウェア クライアント認証またはハードウェア クライアントの個別ユーザ認証には適用されません。

IPSec-UDP アトリビュートの設定

IPSec over UDP（NAT 経由の IPSec）を使用すると、Cisco VPN クライアントまたはハードウェア クライアントが、NAT を実行しているセキュリティ アプライアンスに UDP を経由して接続できるようになります。デフォルトでは無効になっています。IPSec over UDP は独自機能です。リモート アクセス接続にのみ適用され、モード設定が必要です。セキュリティ アプライアンスは、SA のネゴシエート中に設定パラメータをクライアントと交換します。IPSec over UDP を使用すると、システム パフォーマンスがやや低下することがあります。

IPSec over UDP を有効または無効にするには、Inherit チェックボックスをクリアし、**Enable** または **Disable** を選択します。

Cisco VPN クライアントも IPSec over UDP を使用するように設定する必要があります（デフォルトで、使用するように設定されています）。VPN 3002 の場合は、IPSec over UDP を使用するように設定する必要はありません。

IPSec over UDP を使用するには、IPSec over UDP で使用する UDP ポート番号を設定する **IPSec over UDP Port** アトリビュートも設定する必要があります。IPSec ネゴシエーションで、セキュリティ アプライアンスは設定されたポートを傍受し、他のフィルタ ルールで UDP トラフィックがドロップされる場合でも、このポートに UDP トラフィックを転送します。IPSec over UDP Port アトリビュートを設定するには、Inherit チェックボックスをクリアし、フィールドにポート番号を入力します。ポート番号の範囲は 4001 ～ 49151 で、デフォルトのポート値は 10000 です。

IPSec バックアップ サーバの設定

バックアップ サーバを使用する場合は、設定します。IPSec バックアップ サーバを使用すると、プライマリ セキュリティ アプライアンスが使用できなくなったときに、VPN クライアントが中央サイトに接続できるようになります。バックアップ サーバを設定した場合、セキュリティ アプライアンスは、IPSec トンネルが確立されたときにサーバ リストをクライアントにプッシュします。バックアップ サーバは、クライアントまたはプライマリ セキュリティ アプライアンスで設定しない限り存在しません。

バックアップ サーバは、クライアントまたはプライマリ セキュリティ アプライアンスで設定します。バックアップ サーバをセキュリティ アプライアンスで設定した場合、バックアップ サーバ ポリシーがグループ内のクライアントにプッシュされ、クライアントで設定されていたバックアップ サーバ リストがあった場合、これを置き換えます。

（注） ホスト名を使用する場合、プライマリ DNS および WINS サーバとは別のネットワークにバックアップ DNS および WINS サーバを置くことをお勧めします。別に置かなかった場合、ハードウェア クライアントの後ろにあるクライアントが DHCP 経由でハードウェア クライアントから DNS および WINS 情報を取得し、プライマリ サーバへの接続が失われ、バックアップ サーバに別の DNS および WINS 情報があるときに、DHCP リースの期限が切れるまでクライアントはアップデートできません。また、ホスト名を使用していて DNS サーバが使用不能になった場合、大きな遅延が発生することがあります。

バックアップ サーバを指定する、またはクライアント設定から設定済みのバックアップ サーバを削除するには、次の手順を実行します。

ステップ 1　Inherit チェックボックスをクリアします。

ステップ 2　ドロップダウン メニューから、次のオプションのいずれかを選択します。

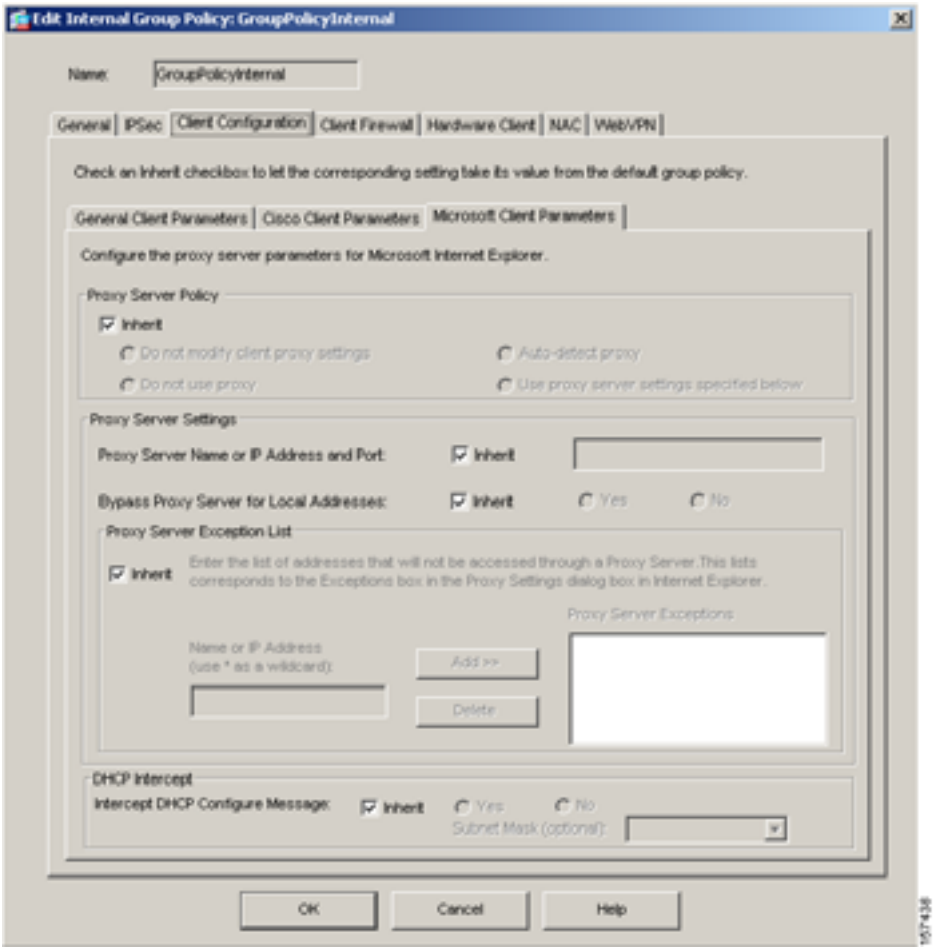
- Keep Client Configuration：セキュリティ アプライアンスがバックアップ サーバ情報をクライアントに送信しないように指定します。クライアントは、独自のバックアップ サーバ リストを使用します（設定されている場合）。これがデフォルトです。
- Clear Client Configuration：クライアントがバックアップ サーバを使用しないように指定します。セキュリティ アプライアンスは、ヌルのサーバ リストをプッシュします。
- Use the Backup Servers Below：プライマリ セキュリティ アプライアンスが使用不能になった場合に使用するサーバのリストを設定することを指定します。

ステップ 3　Use the Backup Servers Below を選択した場合は、Server Addresses フィールドに 1 つ以上のサーバ アドレスを入力する必要があります。このリストは、プライマリ セキュリティ アプライアンスが使用不能になったときに VPN クライアントが使用するサーバを空白で区切り、優先順位の高い順に並べたリストです。このリストは、サーバを IP アドレスまたはホスト名で識別します。リストの長さは 500 文字までで、含めることができるエントリは 10 までです。

Microsoft クライアント パラメータの設定

Microsoft Client Parameters タブ（図 2-30）では、Microsoft クライアントに固有のクライアント アトリビュート（特に、Microsoft Internet Explorer 用のプロキシ サーバ パラメータ）を設定します。

図 2-30　Microsoft Client Parameters タブ



このタブのフィールドを使用して、Microsoft クライアントに固有のパラメータを設定します。

- Proxy Server Policy：クライアント PC の Microsoft Internet Explorer ブラウザのプロキシ アクション（「メソッド」）を設定します。
  - Do not modify client proxy settings：このクライアント PC の Internet Explorer の HTTP ブラウザ プロキシ サーバ設定を変更しません。

- Do not use proxy：クライアント PC の Internet Explorer の HTTP プロキシ設定を無効にします。
- 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有効にします。
- 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。

• 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。

- Proxy Server Name or IP Address：このクライアント PC に適用する Microsoft Internet Explorer サーバの IP アドレスまたは名前を指定します。

（注） ASDM を使用して、プロキシ サーバ名または IP アドレスを設定できます。サーバのほかに使用するオプションのポートを設定するには、group-policy　設定モードで **msie-proxy server** コマンドを使用する必要があります。

- Bypass Proxy Server for Local Addresses：クライアント PC 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 バイパスが有効になり、No を選択するとローカル バイパスが無効になります。
- Proxy Server Exception List：クライアント PC のローカル バイパス用 Microsoft Internet Explorer ブラウザ プロキシ例外リスト設定値を設定します。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の Exceptions ボックスに対応します。
- Name or IP Address (use * as a wildcard)：このクライアント PC に適用する MSIE サーバの IP アドレスまたは名前を指定します。
- Add：指定した名前または IP アドレスを Proxy Server Exceptions 例外リストに追加します。
- Delete：指定した名前または IP アドレスを Proxy Server Exceptions リストから削除します。
- Proxy Server Exceptions：プロキシ サーバ アクセスから除外するサーバ名および IP アドレスをリストします。このリストは、Internet Explorer の Proxy Settings ダイアログボックスの Exceptions ボックスに対応します。

• DHCP Intercept：DHCP 代行受信を有効または無効にします。DHCP 代行受信を使用すると、Microsoft XP クライアントがセキュリティ アプライアンス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。セキュリティ アプライアンスは、Microsoft Windows XP クライアントの DHCP Inform メッセージに直接応答し、トンネル IP アドレスのサブネット マスク、ドメイン名、クラスレス スタティック ルートをクライアントに提供します。XP 以前の Windows クライアントでは、DHCP 代行受信はドメイン名とサブネット マスクを提供します。この機能は、DHCP サーバを使用する利点がない環境で役立ちます。

（注） Microsoft XP では、スプリット トンネル オプションが 255 バイトを超えると、ドメイン名の衝突が不正に発生します。この問題を回避するために、セキュリティ アプライアンスは、送信するルート数を 27 ～ 40 ルートに制限します。このルート数は、ルートのクラスによって異なります。

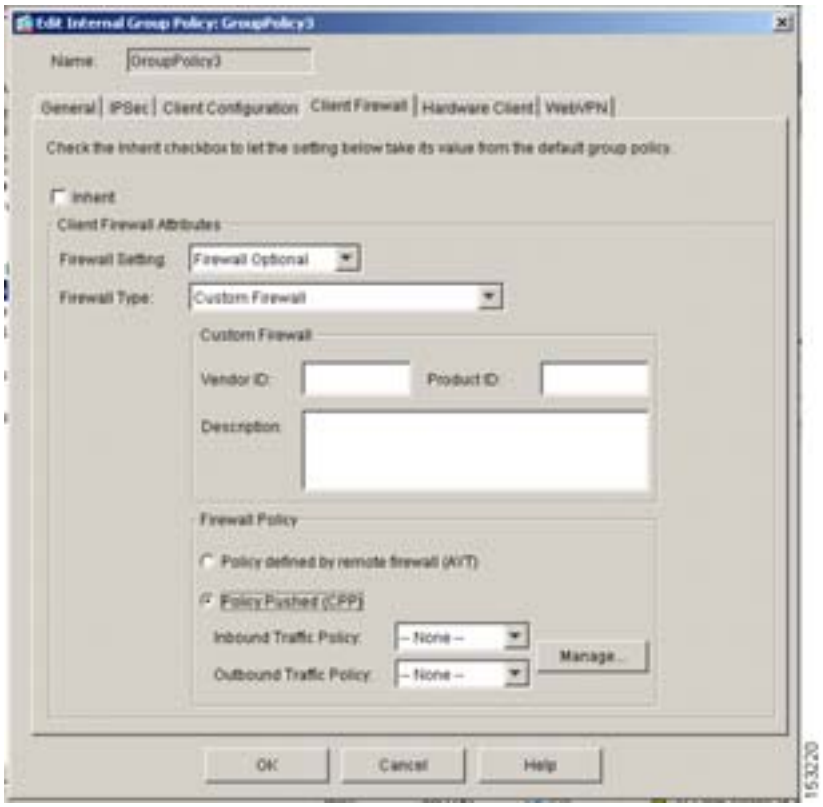
- Intercept DHCP Configure Message：グループ ポリシーから DHCP 代行受信ポリシーを継承するか、DHCP ポリシーを有効（Yes）または無効（No）にするかを指定します。
- Subnet Mask (optional)：ドロップダウン リストからサブネット マスクを選択します。

ファイアウォール アトリビュートの設定

*ファイアウォール*は、インバウンドおよびアウトバウンドの各データ パケットを検査し、許可するかドロップするかを判断することによって、コンピュータをインターネットから隔離し、保護します。ファイアウォールは、グループのリモート ユーザにスプリット トンネリングが設定されている場合に、追加のセキュリティを提供します。この場合、ファイアウォールによってインターネットまたはユーザのローカル LAN からの侵入からユーザの PC が保護され、その結果として、企業のネットワークが保護されます。VPN クライアントでセキュリティ アプライアンス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。ファイアウォール ポリシーがない場合、ユーザは、デフォルト グループ ポリシーまたは他のグループ ポリシーのポリシーを継承できます。

Client Firewall タブ（図 2-31）で、IKE トンネル ネゴシエーション中にセキュリティ アプライアンスが VPN クライアントにプッシュするパーソナル ファイアウォール ポリシーを設定します。

図 2-31　Edit Internal Group Policy Client Firewall タブ



(注)　これらのファイアウォール機能は、Microsoft Windows を実行している VPN クライアントでのみ使用できます。現在、ハードウェア クライアントまたはその他の（非 Windows）ソフトウェア クライアントでは使用できません。

次の例で、クライアント ファイアウォールの使用について説明します。

最初のシナリオでは、リモート ユーザの PC 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るように監視します。ファイアウォールが実行を停止した場合、VPN クライアントはセキュリティ アプライアンスへの接続をドロップします（このファイアウォール適用メカニズムを *Are You There（AYT）*と呼びます。これは、VPN クライアントが定期的に「are you there?」メッセージを送信してファイアウォールを監視するためです。応答が返らなかった場合、VPN クライアントはファイアウォールがダウンしたことを認識し、セキュリティ アプライアンスへの接続を終了します）。これらの PC ファイアウォールは、ネットワーク管理者が最初に設定できますが、この方法で、各ユーザが独自の設定にカスタマイズできます。

2 番目のシナリオでは、VPN クライアント PC にパーソナル ファイアウォールの集中的なファイアウォール ポリシーを適用します。一般的な例として、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例があります。この方法で、トンネルが確立されている間、インターネットからの侵入から PC を保護し、結果として、中央サイトを保護します。このファイアウォール 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。セキュリティ アプライアンスで、トラフィック管理ルールのセットを作成し、VPN クライアントに適用し、これらのルールをフィルタに関連付け、そのフィルタをファイアウォール ポリシーとして指定します。セキュリティ アプライアンスは、このポリシーを VPN クライアントにプッシュします。次に、VPN クライアントが、ポリシーをローカル ファイアウォールに渡して適用します。

Add Internal Group Policy または Edit Internal Group Policy ウィンドウの Client Firewall タブを使用して、追加または修正するグループ ポリシーの VPN クライアントのファイアウォール設定値を設定できます。クライアント ファイアウォール設定値を指定するには、Inherit チェックボックスをクリアし、Client Firewall Attributes 領域で次のアトリビュートを設定します。

ファイアウォール設定値の設定

ドロップダウン メニューから適切な設定を選択して、ファイアウォールがないか、オプションか、必須かを指定します。

（注） 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。

ファイアウォール タイプの設定

ドロップダウン メニューから、ファイアウォールのタイプ（またはファイアウォールなし）を選択します。オプションは次のとおりです。

- No Firewall：クライアント ファイアウォール ポリシーがなく、デフォルト グループ ポリシーまたは特定のグループ ポリシーから継承しないことを示します。
- Cisco Integrated Firewall：Cisco Integrated Firewall タイプを選択します。
- Cisco Security Agent：Cisco Intrusion Prevention Security Agent ファイアウォール タイプを選択します。

- Zone Labs Firewalls：Zone Labs Zone Alarm ファイアウォール タイプ、Zone Alarm Pro ファイアウォール タイプ、またはその両方を選択します。
- Sygate Personal Firewalls：Sygate Personal ファイアウォール タイプ、Sygate Personal Pro ファイアウォール タイプ、または Sygate Security Agent ファイアウォール タイプを選択します。
- Network ICE, Black ICE Firewall：Network ICE Black ICE ファイアウォール タイプを選択します。
- Custom Firewall：このポリシーで、カスタム ファイアウォールを使用することを示します。これを選択すると、Custom Firewall and Firewall Policy 領域がアクティブになります。

カスタム ファイアウォールの設定

ファイアウォール タイプとして Custom Firewall を選択した場合は、次のカスタム ファイアウォール アトリビュートも設定する必要があります。

- Vendor ID：ファイアウォール ベンダーを識別します。
- Product ID：ファイアウォール製品のモデル名または製品名を識別します。
- Description：オプションで、カスタム ファイアウォールの追加情報を指定します。

Firewall Policy アトリビュートを設定して、次のように、発信元およびファイアウォール ポリシーの特性を設定します。

- Policy defined by remote firewall (AYT)：リモート ユーザ PC にインストールされたファイアウォールを使用し、接続が確立された後、ファイアウォールを 30 秒ごとにポーリングして実行していることを確認するように指定します。これを「Are You There」または AYT メカニズムと呼びます。ローカル ファイアウォールのファイアウォール ポリシーが、VPN クライアントに適用されます。セキュリティ アプライアンスは、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。
- Policy Pushed (CPP)：VPN クライアント PC のパーソナル ファイアウォールに、集中化されたファイアウォール ポリシーを適用します。このファイアウォール ポリシーはピアからプッシュされるため、「プッシュ ポリシー」または Central Protection Policy と呼ばれます。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。セキュリティ アプライアンスは、Policy Pushed (CPP) ドロップダウン メニュー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、このセキュリティ アプライアンス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。セキュリティ アプライアンス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。セキュリティ アプライアンスではなく 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、セキュリティ アプライアンス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。

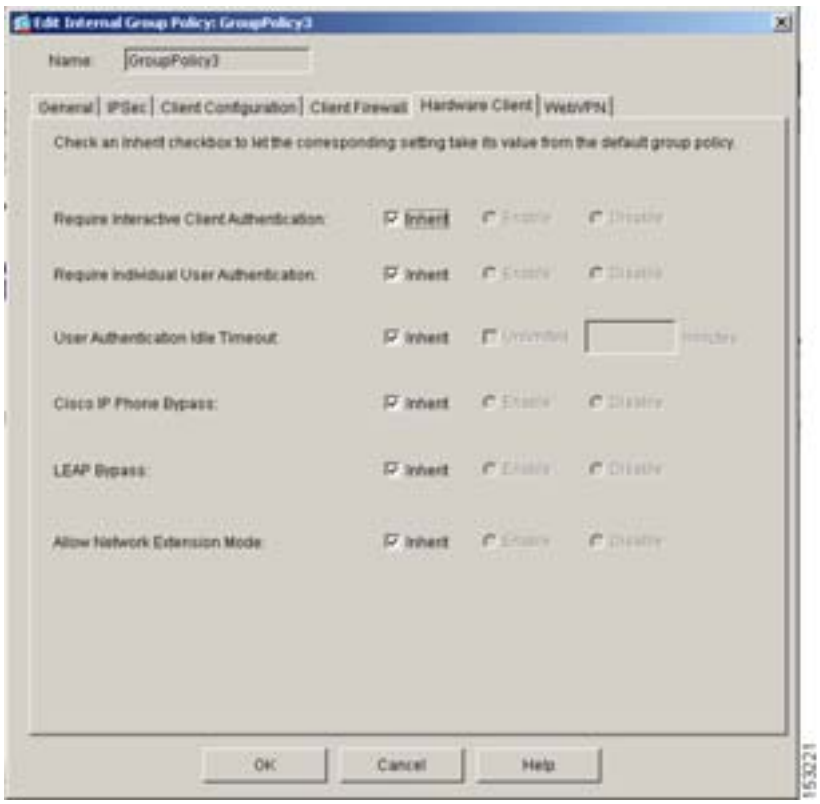
Policy Pushed (CPP) を選択する場合は、クライアントがインバウンドおよびアウトバウンド トラフィックに対して使用するポリシーも選択する必要があります。

Manage をクリックすると、ACL Manager ダイアログボックス（図 2-9）が開きます。このダイアログボックスで、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、これらのルールとフィルタを関連付け、フィルタをファイアウォール ポリシーとして指定できます。セキュリティ アプライアンスは、このポリシーを VPN クライアントにプッシュします。次に、VPN クライアントがポリシーをローカル ファイアウォールに渡し、適用します。

VPN ハードウェア クライアントのアトリビュートの設定

Add Internal Group Policy または Edit Internal Group Policy の Hardware Client タブ（図 2-32）を使用して、VPN ハードウェア クライアントに固有のアトリビュートを設定できます。このタブでは、セキュア ユニット認証およびユーザ認証を有効または無効にでき、VPN ハードウェア クライアントのユーザ認証タイムアウト値を設定できます。また、Cisco IP Phone および LEAP パケットが個別のユーザ認証をバイパスできるようにしたり、ネットワーク拡張モードを使用しているハードウェア クライアントが接続できるようにしたりできます。

図 2-32　Edit Internal Group Policy の Hardware Client タブ



Require Interactive Client Authentication（セキュア ユニット認証）

セキュア ユニット認証は、クライアントがトンネルを開始するたびに、ユーザ名とパスワードによる認証を行うように VPN ハードウェア クライアントに要求することで、追加のセキュリティを提供します。この機能を有効にすると、ハードウェア クライアントはユーザ名とパスワードを保存しません。セキュア ユニット認証は、デフォルトで無効になっています。

（注） この機能を有効にした場合、VPN　トンネルを始動するために、ユーザ名とパスワードを入力するユーザが立ち会う必要があります。

セキュア ユニット認証を使用するには、ハードウェア クライアントが使用するトンネル グループ用に認証サーバ グループを設定しておく必要があります。プライマリ セキュリティ アプライアンスでセキュア ユニット認証を要求する場合は、すべてのバックアップ サーバでも設定する必要があります。

インタラクティブ ハードウェア クライアント認証は、VPN 3002 がトンネルを開始するたびに、手動で入力したユーザ名とパスワードで認証を行うように VPN 3002 ハードウェア クライアントに要求することによって、追加のセキュリティを提供します。この機能を有効にすると、VPN 3002 はユーザ名とパスワードを保存しません。ユーザ名とパスワードを入力すると、VPN 3002 は接続するセキュリティ アプライアンスにクレデンシャルを送信します。セキュリティ アプライアンスは、内部または外部認証サーバを利用して認証を行います。ユーザ名とパスワードが有効な場合、トンネルが確立されます。

グループのインタラクティブ ハードウェア クライアント認証を有効にすると、セキュリティ アプライアンスがグループ内の VPN 3002 にポリシーをプッシュします。以前、VPN 3002 でユーザおよびパスワードを設定していた場合、ソフトウェアによってコンフィギュレーション ファイルから削除されます。接続しようとすると、ソフトウェアによって、ユーザ名とパスワードを要求するプロンプトが表示されます。

後で、セキュリティ アプライアンスでグループのインタラクティブ ハードウェア認証を無効にすると、VPN 3002 でローカルに有効にされ、ユーザ名とパスワードを要求するプロンプトが表示され続けます。これによって、保存されたユーザ名およびパスワードがなく、セキュリティ アプライアンスでインタラクティブ ハードウェア クライアント認証が無効にされても、VPN 3002 は接続できます。後で、ユーザ名とパスワードを設定し、機能を無効にすると、プロンプトは表示されなくなります。VPN 3002 は、保存されたユーザ名とパスワードを使用して、セキュリティ アプライアンスに接続します。

Inherit チェックボックスをクリアし、**Enable** または **Disable** を選択して、インタラクティブ クライアント認証の要求を有効にするか無効にするかを指定します。このパラメータはデフォルトで無効になっています。

Require Individual User Authentication

この機能を有効にすると、トンネルを介してネットワークにアクセスする場合に、ユーザ認証でハードウェア クライアントの後ろにいる個別のユーザの認証が要求されます。個別のユーザは、設定した認証サーバの順序に従って認証されます。これらのユーザの個別ユーザ認証はデフォルトで無効になっています。グループ内の VPN 3002 デバイスにバナーを表示するには、個別ユーザ認証を有効にする必要があります。

プライマリ セキュリティ アプライアンスで個別ユーザ認証を要求する場合は、すべてのバックアップ サーバでも設定する必要があります。

個別ユーザ認証は、VPN 3002 のプライベート ネットワークの認証されないユーザが中央サイトにアクセスできないように保護します。個別ユーザ認証を有効にした場合、VPN 3002 を介して接続する各ユーザは、トンネルがすでに存在していても、Web ブラウザを開いて手動で有効なユーザ名とパスワードを入力し、セキュリティ アプライアンスの後ろにあるネットワークにアクセスする必要があります。

(注) ユーザ認証を有効にした場合、コマンドライン インターフェイスを使用してログインすることはできません。ブラウザを使用する必要があります。

セキュリティ アプライアンスの後ろにあるリモート ネットワークがデフォルト ホームページの場合、または、セキュリティ アプライアンスの後ろにあるリモート ネットワークの Web サイトをブラウザで開く場合、VPN 3002 は、ユーザ ログイン用の適切なページをブラウザで開きます。正常にログインすると、元々入力していたページがブラウザに表示されます。

セキュリティ アプライアンスの後ろにあるネットワークにある Web ベースではないリソース（電子メールなど）にアクセスしようとすると、ブラウザを使用して認証を行うまで、接続に失敗します。

認証を行うには、ブラウザの Location フィールドまたは Address フィールドに、VPN 3002 のプライベート インターフェイスの IP アドレスを入力する必要があります。次に、ブラウザは、VPN 3002 のログイン画面を表示します。認証を行うには、Connect/Login Status ボタンをクリックします。

1 人のユーザは、同時に最大 4 セッションのログインを実行できます。個別のユーザは、グループに対して設定した認証サーバの順序に従って認証されます。

アイドル タイムアウトの設定

ハードウェア クライアントの後ろにいる個別のユーザにアイドル タイムアウトを設定するには、Inherit チェックボックスをクリアし、Unlimited チェックボックスを選択してアイドル タイムアウトなしを指定するか、分単位で特定の数値を指定します。アイドル タイムアウトの時間内にハードウェア クライアントの後ろにいるユーザによる通信アクティビティがない場合、セキュリティ アプライアンスは、そのクライアントのアクセスを終了します。

（注） **user-authentication-idle-timeout** コマンドは、VPN トンネル経由のクライアント アクセスを終了するだけで、VPN トンネル自体は終了しません。

minutes フィールドで、アイドル タイムアウトの時間を分単位で指定します。最小は 1 分、デフォルトは 30 分、最大は 35791394 分です。Inherit チェックボックスと Unlimited チェックボックスの両方をクリアした場合は、minutes フィールドに値を指定する必要があります。

IP Phone バイパスの設定

Cisco IP Phone が、ハードウェア クライアントの後ろにいる個別のユーザの認証をバイパスするようにできます。IP Phone バイパスを有効または無効にするには、Inherit チェックボックスをクリアし、**Enable** または **Disable** を選択します。IP Phone バイパスによって、ハードウェア クライアントの後ろにある IP Phone は、ユーザ認証プロセスを経由せずに接続できるようになります。デフォルトでは、IP Phone バイパスは無効になっています。有効にした場合、セキュア ユニット認証は有効のままです。

（注） IP Phone 接続にネットワーク拡張モードを使用するように、VPN 3002 を設定する必要があります。

LEAP バイパスの設定

VPN 3002 の後ろにいる LEAP ユーザには、面倒な問題があります。トンネルで中央サイト デバイスの後ろにある RADIUS サーバにクレデンシャルを送信することができないため、LEAP 認証をネゴシエートできません。トンネル経由でクレデンシャルを送信できない理由は、無線ネットワークで認証されていないためです。この問題を解決するために、LEAP バイパスは、個別のユーザ認証の前に LEAP パケット（LEAP パケットだけ）をトンネルで転送し、RADIUS サーバへの無線接続を認証できるようにします。これによって、ユーザは、個別のユーザ認証に進むことができます。

LEAP バイパスは、次の条件下で、意図されたとおりに機能します。

- インタラクティブ ユニット認証機能（有線デバイス用）が、無効であること。インタラクティブ ユニット認証が有効の場合、トンネルを使用して LEAP デバイスが接続できるようになる前に、非 LEAP（有線）デバイスが VPN 3002 を認証する必要があります。
- 個別のユーザ認証が有効であること（有効でない場合、LEAP バイパスを使用する必要はありません）。
- 無線環境のアクセス ポイントが Cisco Aironet Access Point であること。PC の NIC カードは、他のブランドの製品でもかまいません。
- Cisco Aironet Access Point で、Cisco Discovery Protocol（CDP）を実行していること。
- VPN 3002 が、クライアント モードまたはネットワーク拡張モードで動作していること（どちらでもかまいません）。
- LEAP パケットが、ポート 1645 または 1812 経由で RADIUS サーバへのトンネルに転送されること。

LEAP バイパスが有効の場合、VPN 3002 ハードウェア クライアントの後ろにある無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルに転送されます。このアクションによって、Cisco 無線アクセス ポイント デバイスを使用しているワークステーションは、LEAP 認証を確立してから、もう一度ユーザごとの認証を行います（有効の場合）。デフォルトでは、LEAP バイパスは無効になっています。

Cisco 無線アクセス ポイントからの LEAP パケットが個別のユーザ認証をバイパスできるようにするには、Inherit チェックボックスをクリアして、**Enable** を選択します。LEAP バイパスを無効にするには、**Disable** を選択します。

（注） IEEE 802.1X は、有線および無線ネットワークの認証の規格です。この規格は、クライアントと認証サーバの間の強力な相互認証を無線 LAN に提供します。ユーザごと、セッションごとのダイナミック WEP（wireless encryption privacy）鍵を提供することで、スタティック WEP 鍵で発生する管理作業とセキュリティ上の問題を軽減します。

シスコシステムズでは、Cisco LEAP という 802.1X 無線認証タイプを開発しています。LEAP（Lightweight Extensible Authentication Protocol）は、接続の一方の無線クライアントと他方の RADIUS サーバとの間で、相互認証を実装します。認証に使用されるクレデンシャル（パスワードを含む）は、無線メディアで転送される前に必ず暗号化されます。

Cisco LEAP は、RADIUS サーバに対して無線クライアントを認証します。RADIUS アカウンティング サーバは含まれません。

この機能は、インタラクティブ ハードウェア クライアント認証が有効の場合、意図されたとおりに機能しません。

注意 認証されていないトラフィックをトンネルで伝送できるようにすると、ネットワークにセキュリティ上のリスクをもたらす可能性があります。

ネットワーク拡張モードの有効化

ネットワーク拡張モードによって、ハードウェア クライアントは、単一のルート指定可能なネットワークを VPN トンネル経由でリモート プライベート ネットワークに提供できます。IPSec は、ハードウェア クライアントの後ろにあるプライベート ネットワークからセキュリティ アプライアンスの後ろにあるネットワークへのすべてのトラフィックをカプセル化します。PAT は適用されません。そのため、セキュリティ アプライアンスの後ろにあるデバイスは、ハードウェア クライアントの後ろにあるプライベート ネットワークのデバイスに、トンネル経由で（必ずトンネル経由で）直接アクセスできます。逆方向のアクセスも同様に可能です。ハードウェア クライアントがトンネルを開始する必要がありますが、トンネルが開始した後は、どちらの側からもデータの交換を開始できます。

Call Manager は実際の IP アドレスでのみ通信できるため、VPN 3002 が IP Phone 接続をサポートするには、ネットワーク拡張モードが必要です。

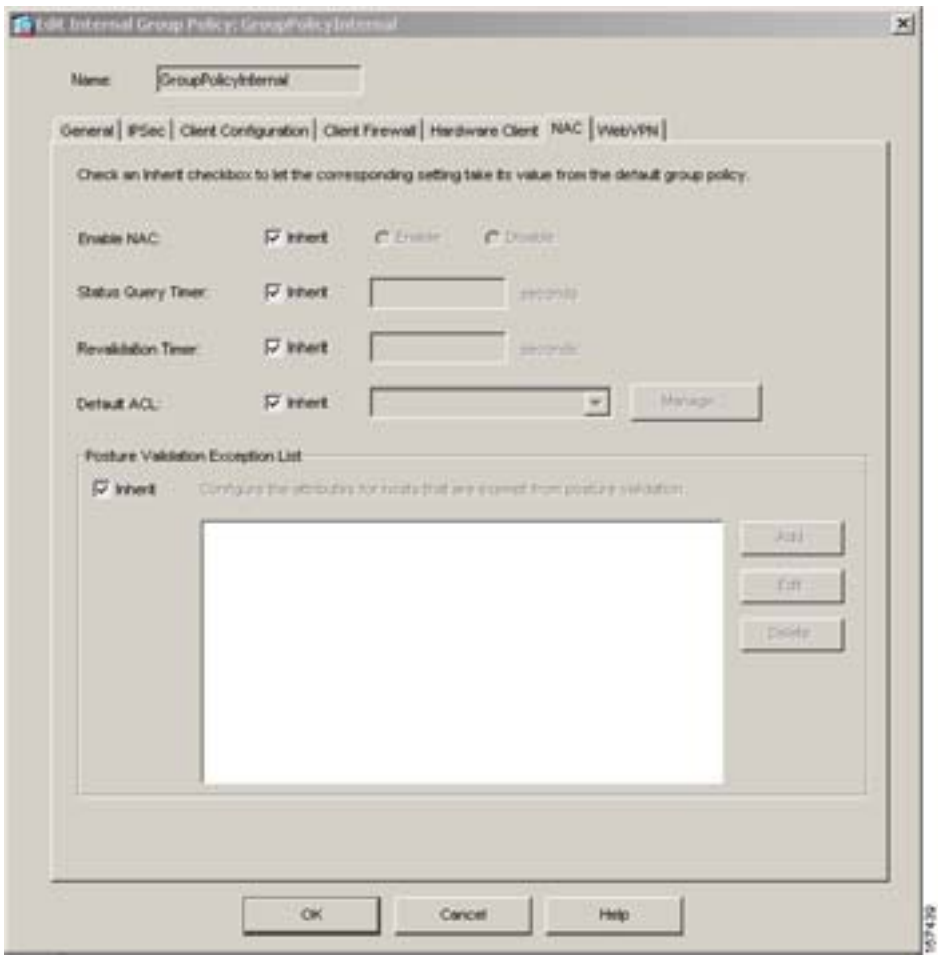
（注） ネットワーク拡張モードを禁止すると（デフォルト設定）、VPN 3002 はこのセキュリティ アプライアンスに PAT モードでのみ接続できるようになります。ここでネットワーク拡張モードを禁止するときは、グループ内のすべての VPN 3002 を PAT モード用に設定してください。ネットワーク拡張モードを使用するように VPN 3002 が設定されていて、接続しようとするセキュリティ アプライアンスがネットワーク拡張モードを禁止している場合、VPN 3002 は 4 秒ごとに接続を試行し、すべての試行が拒否されます。この場合、VPN 3002 は、接続しようとするセキュリティ アプライアンスに不要な処理負荷をかけることになります。多数の VPN 3002 がこのように誤設定されている場合、セキュリティ アプライアンスのサービス提供能力が損なわれます。

ハードウェア クライアントのネットワーク拡張モードを有効または無効にするには、Inherit チェックボックスをクリアし、**Enable** または **Disable** を選択します。

ネットワーク アドミッション コントロールの設定

Add Internal Group Policy または Edit Internal Group Policy ウィンドウの NAC タブ（図 2-33）を使用して、デフォルト グループ ポリシーまたは代替グループ ポリシーのネットワーク アドミッション コントロールの設定値を設定できます。

図 2-33　NAC タブ



このタブのすべてのパラメータは、デフォルトとして、デフォルト グループ ポリシーから値を継承するように設定されています。明示的に設定するパラメータの Inherit チェックボックスをクリアします。このウィンドウのフィールドは、次のとおりです。

- Inherit：（複数インスタンス）対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。このタブのすべてのアトリビュートのデフォルト設定です。
- Enable NAC：リモート アクセスに対してポスチャ検証を要求します。リモート コンピュータが検証チェックをパスした場合、ACS サーバは、セキュリティ アプライアンスが適用するアクセス ポリシーをダウンロードします。デフォルト設定は Disable です。
- Status Query Timer：セキュリティ アプライアンスは、ポスチャ検証とステータス クエリの応答が成功するたびに、このタイマーを開始します。このタイマーの有効期限が過ぎると、ホスト ポスチャの変化を問い合せるクエリ（*ステータス クエリ*）が発行されます。秒単位で、30 ～ 1800 の数値を入力します。デフォルト設定は 300 です。
- Revalidation Timer：セキュリティ アプライアンスは、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。このタイマーの有効期限が過ぎると、次の無条件ポスチャ検証が実行されます。セキュリティ アプライアンスは、再検証の間、ポスチャ検証を維持します。ポスチャ検証または再検証の際に Access Control Server が使用できない場合、デフォルト グループ ポリシーが有効になります。成功したポスチャ検証の間隔とする時間を秒単位で入力します。範囲は 300 ～ 86400 です。デフォルト設定は 36000 です。

- Default ACL：（オプション）ポスチャ検証が失敗した場合、セキュリティ アプライアンスは、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、セキュリティ アプライアンスはデフォルト 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、有効化、無効化、削除します。Default ACL アトリビュートの横のリストに ACL が表示されます。
- 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 つ以上のアトリビュートが表示されます。少なくとも、エントリごとにオペレーティング システムと Enabled 設定（Yes または No）が表示されます。オプションのフィルタによって、リモート コンピュータの追加のアトリビュートと一致する 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。セキュリティ アプライアンスは、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。

グループ ポリシーの WebVPN アトリビュートの設定

WebVPN を使用すると、ユーザが Web ブラウザを使用して、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るようになります。ソフトウェアまたはハードウェア クライアントは必要ありません。WebVPN は、HTTPS インターネット サイトに到達できるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできるようにします。WebVPN は、SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされる内部リソースとの間に、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシ処理が必要な接続を認識し、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。デフォルトでは、WebVPN は無効になっています。

特定の内部グループ ポリシー用に、WebVPN 設定をカスタマイズできます。

Add Internal Group Policy または Edit Internal Group Policy の WebVPN タブで、すべての機能の設定を継承するか、WebVPN アトリビュートをカスタマイズするかを指定できます。次の項で、各アトリビュートについて説明します。

- Functions
- Content Filtering
- Homepage
- Port Forwarding
- Other（サーバ リスト、URL リストなど）
- SSL VPN Client（SVC）
- Auto Signon

多くの場合、WebVPN アトリビュートは、WebVPN の設定の一部として定義します。その後、group-policy webvpn アトリビュートを設定するときに、これらの定義を特定のグループに適用します。グループ ポリシーの WebVPN タブのアトリビュートは、WebVPN 経由でのファイル、MAPI プロキシ、URL、および TCP アプリケーションへのアクセスを定義します。また、ACL およびフィルタするトラフィックのタイプも識別します。WebVPN は、デフォルトで無効になっています。

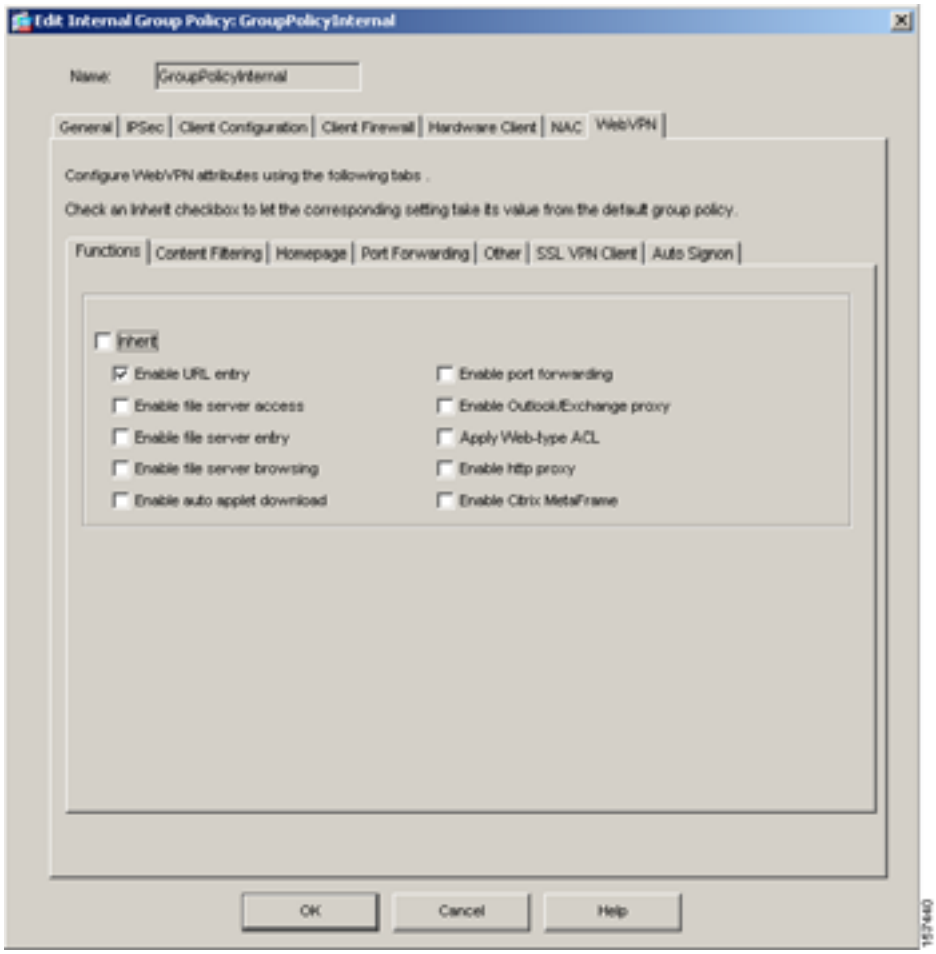
WebVPN アトリビュートの設定に関する詳細については、このタブのオンライン ヘルプの WebVPN の説明、『*Cisco Security Appliance Command Line Configuration Guide*』、および『*Cisco Security Appliance Command Reference*』を参照してください。

電子メール プロキシを使用するために、WebVPN を設定する必要はありません。

グループ ポリシーの WebVPN Function タブ アトリビュートの設定

Functions タブ（図 2-34）を使用して、基本的な WebVPN 機能を設定できます。有効にする WebVPN 機能（ファイル アクセスや、WebVPN 経由のファイル参照、HTTP プロキシ、MAPI プロキシ、URL 入力など）を設定するには、Inherit チェックボックスをクリアし、有効にするまたは適用する個別機能のチェックボックスを選択します。これらの機能は、デフォルトで無効になっています。

図 2-34　Edit Internal Group Policy の WebVPN タブの Functions タブ



このタブで設定できる機能は、次のとおりです。

- Enable URL entry：ユーザによる URL 入力を有効または無効にし、ホームページに URL 入力ボックスを配置します。有効にした場合も、セキュリティ アプライアンスは、設定済み URL またはネットワーク ACL によって URL を制限します。ユーザは URL 入力ボックスに Web アドレスを入力し、WebVPN を使用してこれらの Web サイトにアクセスできます。URL entry を無効にすると、セキュリティ アプライアンスは、WebVPN ユーザがアクセスできる URL をホームページの URL に制限します。

WebVPN を使用しても、すべてのサイトと安全に通信できることは保証されません。WebVPN は、リモート ユーザの PC またはワークステーションと、企業ネットワークのセキュリティ アプライアンスとの間のデータ転送のセキュリティを保証します。ユーザが（インターネットまたは内部ネットワークにある）非 HTTPS Web リソースにアクセスした場合、企業のセキュリティ アプライアンスから目的の Web サーバへの通信は安全ではありません。

WebVPN 接続では、エンド ユーザの Web ブラウザと目的の Web サーバとの間で、セキュリティ アプライアンスはプロキシとして機能します。WebVPN ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュア接続を確立し、サーバの SSL 認証を検証します。エンド ユーザのブラウザは、提供された証明書を受け取らないため、証明書の検査と検証ができません。現在の WebVPN の実装では、有効期限が切れた証明書を提供するサイトとの通信は許可されません。また、セキュリティ アプライアンスは、信頼済み CA 証明書の検証も実行しません。そのため、WebVPN ユーザは、SSL 対応 Web サーバと通信する前に、提供される証明書を分析できません。

WebVPN ユーザのインターネット アクセスを制限するには、Enable URL Entry フィールドを選択解除します。これによって、WebVPN ユーザは、WebVPN 接続中に Web サーフィンができなくなります。

- Enable file server access：HTTPS を介した Windows ファイル アクセス（SMB/CIFS ファイルのみ）を有効または無効にします。有効にすると、WebVPN ホームページのサーバ リストにファイル サーバが表示されます。ファイル閲覧やファイル入力を有効にするには、ファイル アクセスを有効にする必要があります。

  このボックスを選択すると、ユーザはネットワーク上の Windows ファイルにアクセスできるようになります。WebVPN ファイル共有用にこのパラメータだけを有効にした場合、ユーザは Servers and URLs 領域で設定されたサーバにのみアクセスできます（P.2-59 の「WebVPN の Other タブを使用したサーバ引数およびリスト引数の設定」の説明を参照してください）。ユーザがサーバに直接アクセスしたり、ネットワーク上のサーバを参照できるようにするには、Enable file server entry および Enable file server browsing アトリビュートの説明を参照してください。

  このチェックボックスを選択すると、ユーザはファイルのダウンロード、編集、削除、名前変更、移動ができるようになります。ファイルとフォルダの追加もできます。

  適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、ファイルにアクセスする前に、ユーザの認証が必要になります。

  ファイル アクセス、サーバ / ドメイン アクセス、および参照を行うには、WINS サーバまたはマスター ブラウザ（通常、セキュリティ アプライアンスと同じネットワーク、またはそのネットワークから到達可能なネットワークに存在）を設定する必要があります。WINS サーバまたはマスター ブラウザは、セキュリティ アプライアンスにネットワーク上のリソースのリストを提供します。代わりに DNS サーバを使用することはできません。

（注）　ダイナミック DNS を同時に使用している場合、Active Native Directory 環境でファイル アクセスはサポートされません。WINS サーバを同時に使用している場合にサポートされます。

- Enable file server entry：ユーザがファイル サーバ名を入力できるようにするかどうかを決定します。ファイル サーバ入力ボックスは、ポータル ページに配置されます。ファイル サーバ アクセスが有効になっている必要があります。

  このチェックボックスを選択すると、ユーザは Windows ファイルのパス名を直接入力できるようになります。ファイルのダウンロード、編集、削除、名前変更、移動ができます。ファイルとフォルダの追加もできます。ここでも、適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、ファイルにアクセスする前に、ユーザの認証が必要になります。

- Enable file server browsing：Windows ネットワークでのファイル、ドメイン / ワークグループ、ファイル サーバ、および共有の参照を有効または無効にします。ユーザによるファイル サーバの入力を許可するには、ファイル参照を有効にする必要があります。ファイル サーバ アクセスが有効になっている必要があります。

このチェックボックスを選択すると、ユーザがドメインおよびワークグループを選択し、そのドメイン内のサーバおよび共有を参照できるようになります。適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、サーバにアクセスする前に、ユーザの認証が必要になります。

- Enable auto applet download：ユーザが WebVPN にログインしたときに、ポート転送 Java アプレットを自動的にダウンロードし、起動できるようにします。デフォルトでは無効になっています。この機能は、ポート転送、Outlook/Exchange プロキシ、または HTTP プロキシも有効になっている場合にだけ有効にできます。自動アプレット ダウンロードは、デフォルト グループ ポリシー（DfltGrpPolicy）またはユーザ定義のグループ ポリシーでも有効にできます。
- Enable port forwarding：WebVPN ポート転送を使用すると、グループ内のリモート ユーザが既知の固定 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るようになります。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 バージョンでは機能しません。

このチェックボックスを選択すると、ローカルおよびリモート システムの TCP ポートをマッピングすることによって、ユーザがクライアント / サーバ アプリケーションにアクセスできるようになります。

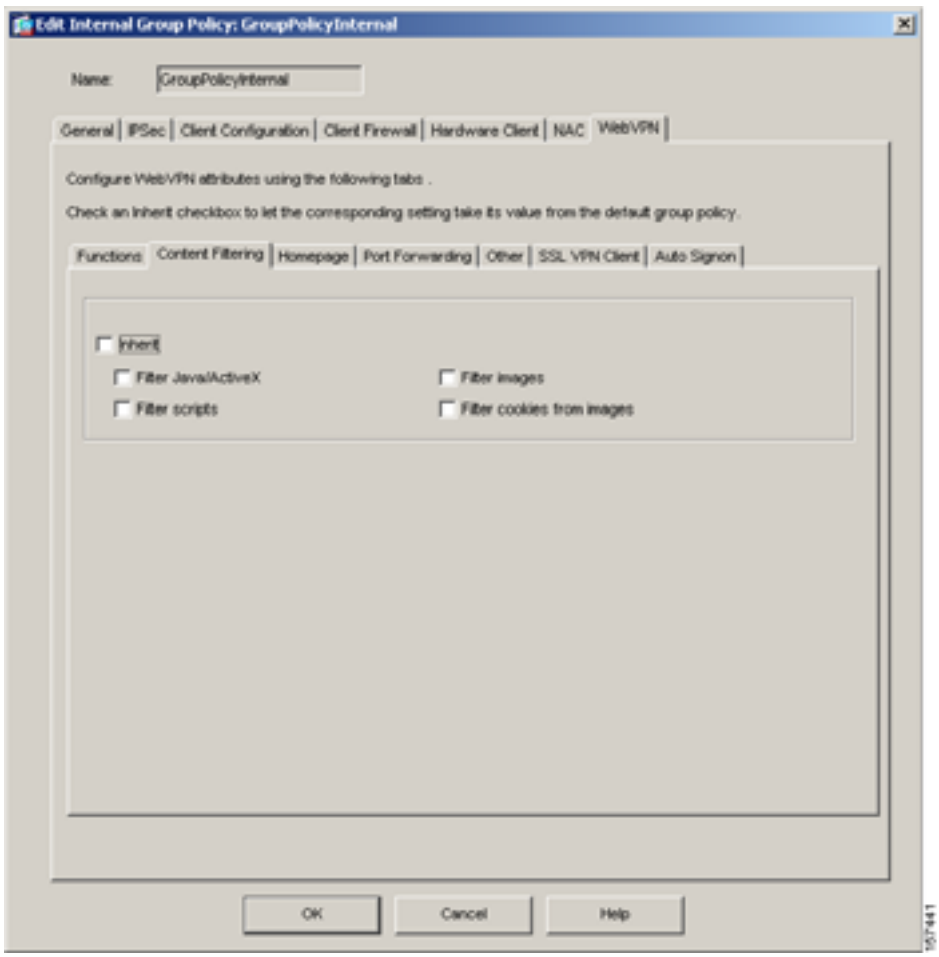
（注） デジタル証明書を使用してユーザを認証する場合、TCP ポート転送 JAVA アプレットは機能しません。JAVA は Web ブラウザのキーストアにアクセスできません。そのため JAVA は、ブラウザがユーザ認証に使用する証明書を使用できず、アプリケーションを起動できません。アプリケーションにアクセスできるようにする場合は、WebVPN ユーザの認証にデジタル証明書を使用しないでください。

- Enable Outlook/Exchange proxy：Microsoft Outlook/Exchange 電子メール プロキシを有効または無効にします。
- Apply Web-type ACL：このグループのユーザに定義した WebVPN アクセス コントロール リストを適用します。
- Enable HTTP proxy：クライアントへの HTTP アプレット プロキシの転送を有効または無効にします。プロキシは、Java、ActiveX、Flash など、適切なコンテンツ トランスフォーム（細分化）と干渉する技術にとって役立ちます。セキュリティ アプライアンスを使用しながら、細分化をバイパスします。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。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、事実上すべてのクライアント サイド テクノロジーをサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。
- Enable Citrix/MetaFrame：MetaFrame Application Server からクライアントへのターミナル サービスのサポートを有効にします。このアトリビュートを使用すると、セキュアな Citrix 設定内でセキュリティ アプライアンスがセキュア ゲートウェイとして機能できるようになります。これらのサービスは、ユーザが MetaFrame アプリケーションに標準 Web ブラウザでアクセスできるようにします。

Content Filtering タブ アトリビュートの設定

Content Filtering タブ（図 2-35）を使用して、Web サイトのうち Java または Active X を使用する部分、スクリプトを使用する部分、画像を表示する部分、および cookie を配信する部分をブロックまたは削除するように、セキュリティ アプライアンスを設定できます。デフォルトでは、これらのパラメータは無効になっていて、フィルタリングは行われません。WebVPN フィルタを設定するには、Inherit チェックボックスをクリアし、有効にする個別のフィルタのチェックボックスを選択します。これらの機能は、デフォルトで無効になっています。

図 2-35　Edit Internal Group Policy の WebVPN タブの Content Filtering タブ



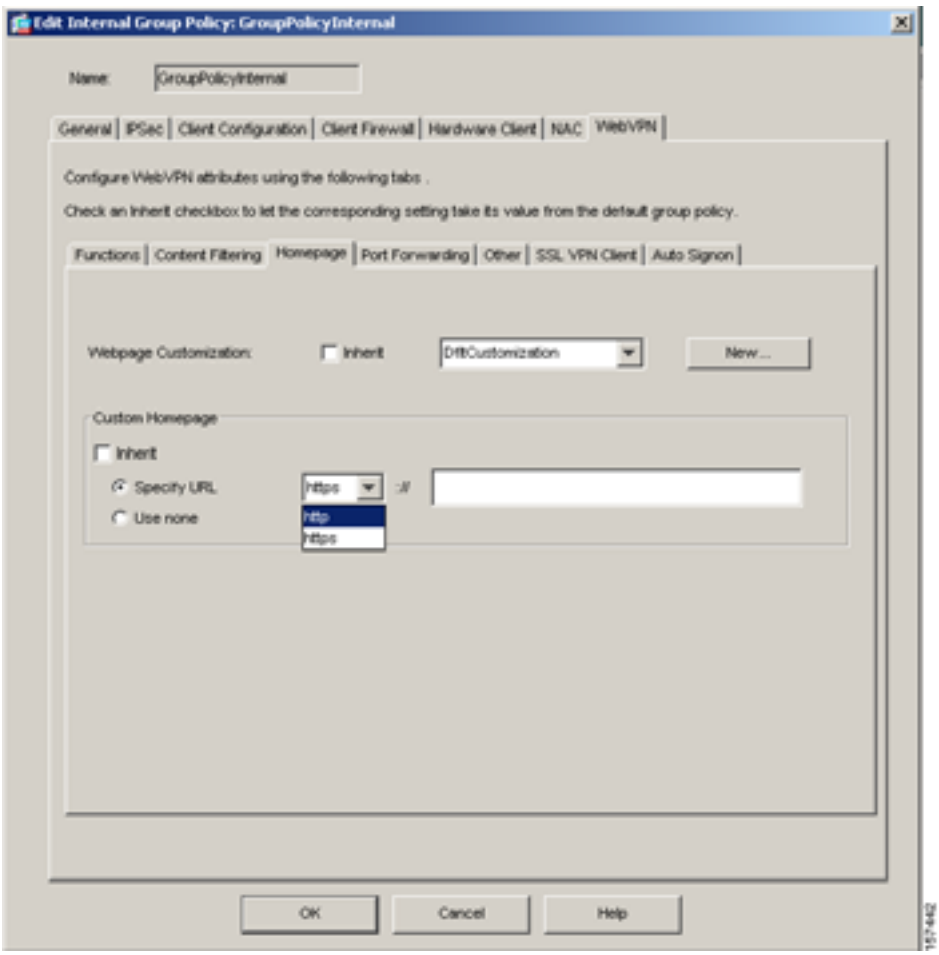
このタブで設定できるフィルタは、次のとおりです。

- Filter Java/ActiveX：Java および ActiveX への参照を削除します。つまり、<applet>、<embed>、および <object> タグを HTML から削除します。
- Filter scripts：スクリプトへの参照を削除します。つまり、<script> タグを HTML から削除します。
- Filter images：<img> タグを HTML から削除します。画像を削除すると、Web ページの配信が大幅に高速化されます。
- Filter cookies from images：画像で配信される cookie を削除します。広告主は cookie を使用して訪問者を追跡するため、これによってユーザのプライバシーが保護されます。

ユーザ ホームページの設定

ASDM を使用して、ユーザがログインしたときに表示されるホームページをカスタマイズできます。ホームページのカスタマイゼーション（色、ロゴなど）は、WebVPN 設定の一部として定義し、特定のグループ ポリシーを設定するときにカスタマイゼーションを適用します。Add Group Policy または Edit Group Policy ウィンドウの WebVPN タブの Homepage タブ（図 2-36）を使用して、ユーザがログインしたときに表示されるホームページを設定できます（ホームページがある場合）。また、ログイン Web ページのルックアンドフィールを変更するために適用する、前に定義したカスタマイゼーションの名前を指定できます。デフォルトのホームページはありません。カスタマイゼーションのデフォルトは、カスタマイゼーションなしです。Web ページ カスタマイゼーション設定の詳細については、Configuration > VPN > WebVPN > Webpage Customization のオンライン ヘルプを参照してください。

図 2-36　Edit Internal Group Policy の WebVPN タブの Homepage タブ



Webpage Customization アトリビュートを指定するには、Inherit チェックボックスをクリアし、ドロップダウン メニューからカスタマイゼーションの名前を選択するか、**New** をクリックして新しいカスタマイゼーションを定義します。**New** をクリックすると、Add Customization Object 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の **Homepage** タブをクリックして、ユーザ ホームページのカスタマイゼーションを設定します。その他のタブでは、ユーザに対して表示するさまざまな GUI ページに適用するその他の Web ページ カスタマイゼーションを設定します。Web ページ カスタマイゼーションの設定方法の詳細については、ダイアログボックスのオンライン ヘルプを参照してください。

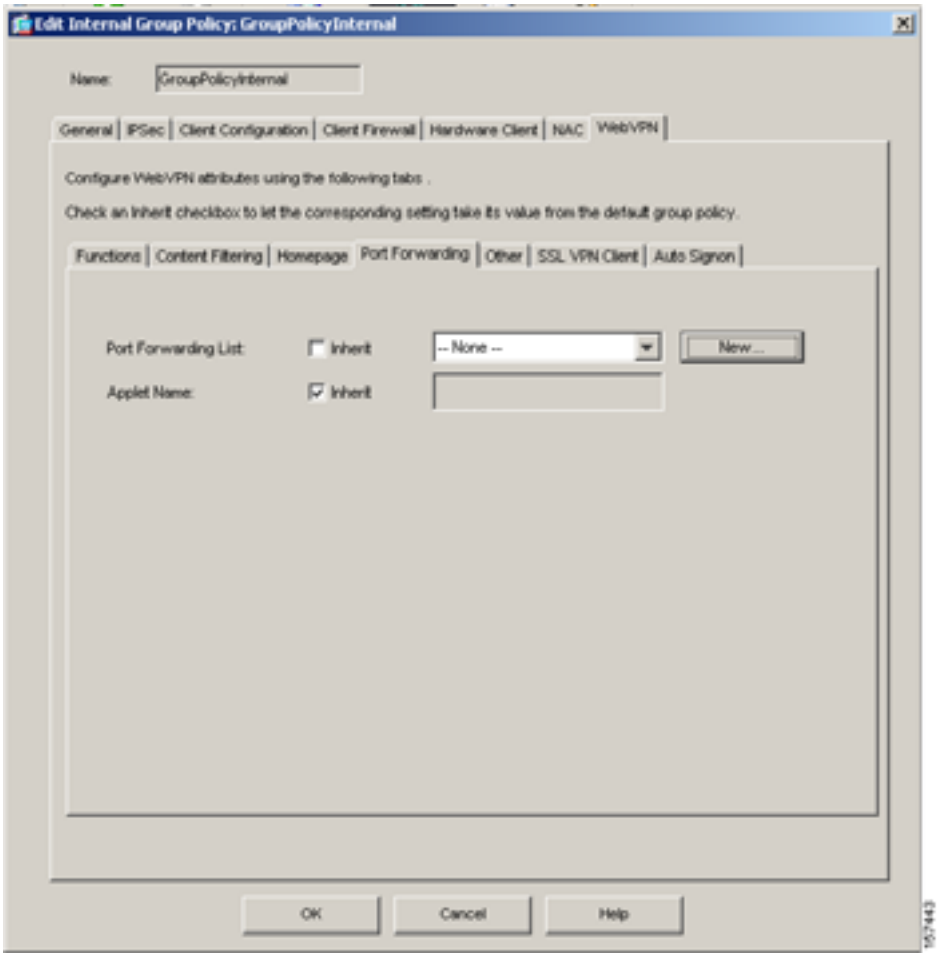
カスタマイゼーションを指定するかどうかにかかわらず、ユーザがログインしたときに表示される特定のホームページを指定できます。デフォルトのホームページはありません。このグループのユーザがログインしたときに表示される Web ページの URL を指定するには、Custom Homepage 領域の Inherit チェックボックスをクリアして、**Specify URL** を選択します。**http** または **https**（デフォルト）を選択して、ホームページの接続プロトコルとして http または https を選択します。文字 :// の右のフィールドで、ホームページとして使用する Web ページの URL を指定します。

設定したホームページを削除するには、**Use None** を選択します。ヌル値が設定され、ホームページが無効になり、継承もされません。

グループ ポリシーのポート転送（WebVPN アプリケーション アクセス）の有効化

ポート転送はアプリケーション アクセスとも呼ばれ、WebVPN ユーザがリモート接続経由でアクセスできるアプリケーションのリストを制御できます。デフォルトでは、ポート転送は無効になっています。Add Group Policy または Edit Group Policy ウィンドウの WebVPN タブの Port Forwarding タブ（図 2-37）を使用して、ポート転送パラメータを設定できます。

図 2-37　Edit Internal Group Policy の WebVPN タブの Port Forwarding タブ

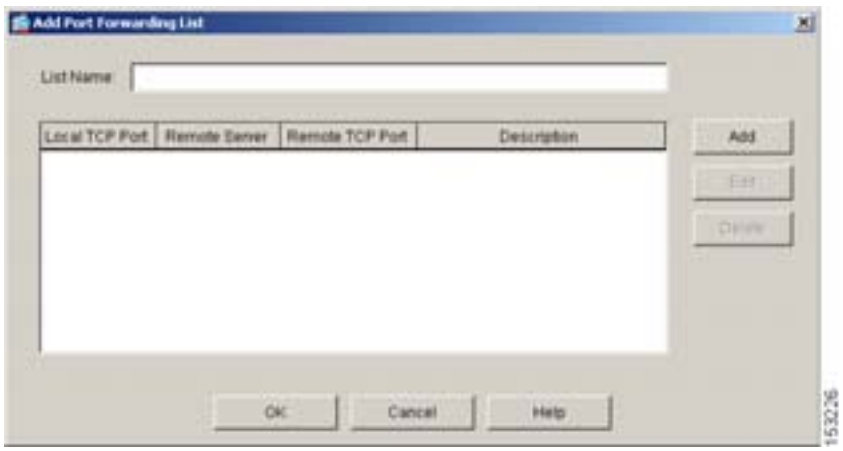


ポート転送で使用できるようにするアプリケーションのリストは、WebVPN 設定の一部として、またはグループ ポリシーの Port Forwarding タブで設定します。ポート転送をグループ ポリシーに適用するには、Inherit チェックボックスをクリアして、次のフィールドを設定します。

- Port Forwarding List：ポート転送リストをデフォルト グループ ポリシーから継承するか、リストから選択するか、新しいポート転送リストを作成するかを指定します。デフォルトは **None** で、ポート転送リストは継承されません。
- 新しいポート転送アプリケーション リストを作成するには、**New** をクリックします。New をクリックすると、新しいポート転送リストを追加できるダイアログボックスが開きます。Add Port Forwarding List または Edit Port Forwarding List ウィンドウの説明を参照してください。
- Applet Name：アプレット名を継承するか、このフィールドで指定した名前を使用するかを指定します。この名前を指定して、エンド ユーザに対してポート転送を識別します。設定した名前は、エンド ユーザ インターフェイスで、ホットリンクとして表示されます。ユーザがこのリンクをクリックすると、Java アプレットによって、設定されているポート転送アプリケーションのリストを表示してアクセスできるようにするウィンドウが開きます。デフォルトのアプレット名は Application Access です。

Add Port Forwarding List または Edit Port Forwarding List ダイアログボックス（図 2-38）を使用して、追加または修正されるグループ ポリシーの WebVPN ユーザの新しいポート転送リスト エントリの設定、または既存のエントリの修正ができます。

図 2-38　Add Port Forwarding List ダイアログボックス



ポート転送リストを追加するには、**Add** をクリックして、次のフィールドを設定します。既存のポート転送リストを編集するには、テーブル領域のリスト エントリを選択して、**Edit** をクリックし、適切なフィールドを設定します。ポート転送エントリをこのリストから削除するには、**Delete** をクリックします。フィールドの説明は次のとおりです。

- List Name：このポート転送リストの名前を指定します。リスト エントリがすでに存在する場合、Add、Edit、および Delete ボタンがアクティブになります。リスト名の下のテーブルには、次のカラムがあります。
- Local TCP Port：このリストのローカル TCP ポートを指定します。
- Remote Server：リモート ピアの名前または IP アドレスを指定します。
- Remote TCP Port：リモート ピアが使用する TCP ポートを指定します。
- Description：このリストの簡単な説明を提供します。

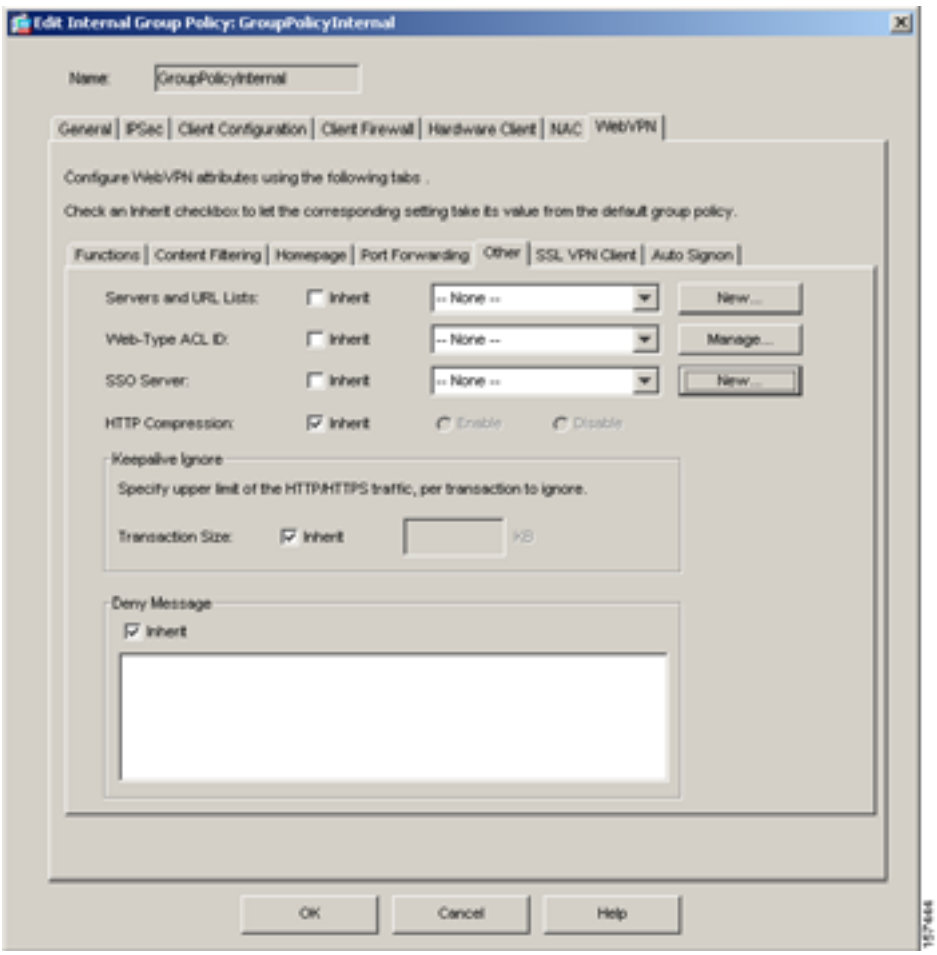
(注)

ポート転送は、スタティック TCP ポートを使用する TCP アプリケーションだけをサポートします。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ません。たとえば、ポート 22 を使用する SecureFTP は WebVPN ポート転送で機能しますが、ポート 20 と 21 を使用する標準 FTP は機能しません。

WebVPN の Other タブを使用したサーバ引数およびリスト引数の設定

Add Group Policy または Edit Group Policy ウィンドウの WebVPN タブの Other タブ（図 2-39）を使用して、サーバと URL のリストおよび Web-type ACL ID を設定できます。

図 2-39　Edit Internal Group Policy の WebVPN タブの Other タブ

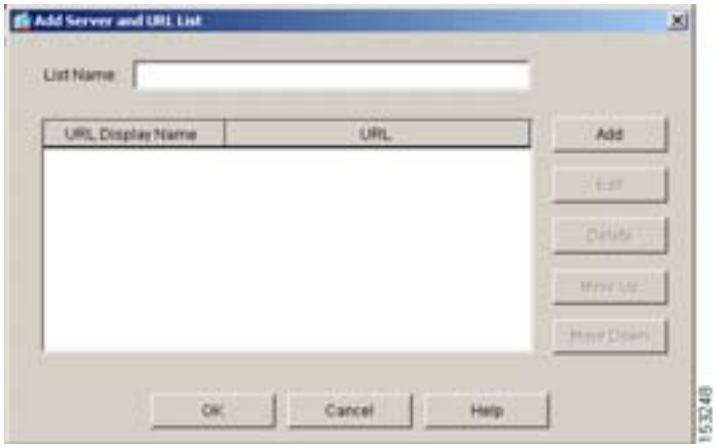


このタブを使用して、次のように、サーバ機能および管理機能の組み合せを設定できます。個別のフィールドを設定するには、そのフィールドの Inherit チェックボックスをクリアします。

- Servers and URL Lists は、サーバおよび URL のリストを継承するか、既存のリストを選択するか、新しいリストを作成するかを指定します。ドロップダウン メニューからリスト名を選択するか、**New** をクリックして Add Server and URL List ダイアログボックス（図 2-40）を開き、新しいサーバまたは URL をリストに追加します。このダイアログボックスで追加した URL 表示名は、Add Internal Group Policy または Edit Internal Group Policy の WebVPN タブの Other タブ

ウィンドウで、Servers and URL Lists 引数のリストに表示されます。URL リストのエントリの順序を変更するには、**Move Up** または **Move Down** をクリックします。デフォルトの URL リストはありません。

図 2-40　Add Server and URL List ダイアログボックス



- ACL を設定して、このグループ ポリシーでさまざまなトラフィック タイプを許可または拒否します。次に、これらの ACL を WebVPN トラフィックに*適用*します。Web-Type ACL ID は、このグループ ポリシーの WebVPN 接続に適用するアクセスリスト名を指定します。Inherit チェックボックスをクリアした場合は、使用する既存の Web-Type ACL の ID を選択するか、Web-Type ACL を追加または修正します。アクセスリストを削除して、フィルタ値の継承も行わないようにするには、ドロップダウン リストから **None** を選択します。
- Manage をクリックすると ACL Manager ダイアログボックス（図 2-9）が開き、Web-Type ACL を管理できます。

  Add ACL、Add ACE、または Edit ACE をクリックすると、ダイアログボックスが開き、対応する機能を実行できます。これらのダイアログボックスのフィールドの詳細については、P.2-13 の「ACL フィルタの設定」を参照してください。

  Web-Type ACL を追加した後で Add ACE をクリックすると、その ACL を設定できます。Add ACE ダイアログボックスが開き、他の ACL および ACE と同様に、アクション（許可 / 拒否）、フィルタ（URL または IP アドレス、サブネット マスク、およびポート）、syslog オプション、および時間範囲名を設定できます。

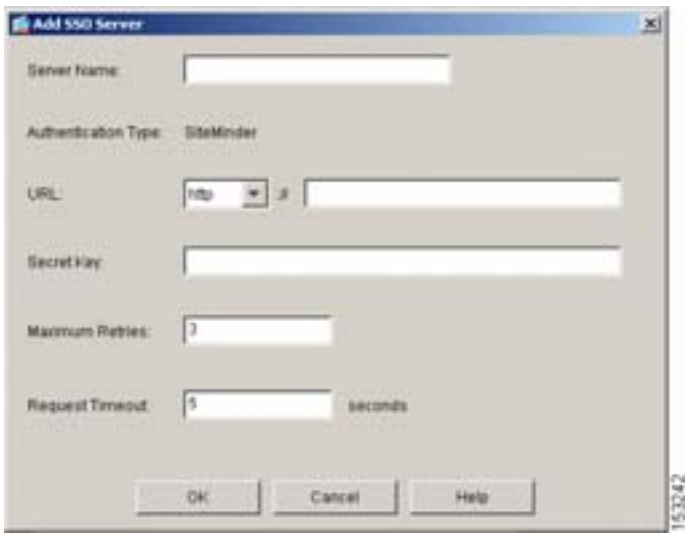
（注） WebVPN で ACL フィルタリングを使用するには、WebVPN-Type ACL をここで定義する必要があります。WebVPN は、ACL Manager で定義された ACL を使用しません。

- **SSO Server** アトリビュートは、シングルサインオン（SSO）サーバ設定を継承するか、既存の SSO サーバをリストから選択するか、新しい SSO サーバを追加するかを指定します。シングルサインオンのサポートは、WebVPN でのみ使用でき、ユーザが複数回ユーザ名とパスワードを入力せずに、異なるサーバの異なるセキュア サービスにアクセスできるようにします。SSO サーバに割り当てられるデフォルト ポリシーは DfltGrpPolicy です。割り当てを削除し、デフォルト ポリシーからの継承を行わないようにするには、ドロップダウン リストから **None** を選択します。

（注） このアトリビュートを使用するには、設定に CA SiteMinder を含める必要があります。

New をクリックすると Add SSO Server ダイアログボックス（図 2-41）が開き、新しいサーバをリストに追加できます。

図 2-41　Add SSO Server



このダイアログボックスのフィールドは、次のように設定します。

- Server Name フィールドでサーバ名を指定します。この名前は、Add Internal Group Policy または Edit Internal Group Policy の WebVPN タブの Other タブで、SSO Server アトリビュートのドロップダウン メニューに表示されます。サーバを追加ではなく編集する場合、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。
- Authentication Type フィールドは表示専用です。SSO サーバのタイプが表示されます。現在、セキュリティ アプライアンスがサポートするタイプは SiteMinder です。
- URL フィールドで、ドロップダウン メニューからプロトコル（http または https）を選択します。次に、セキュリティ アプライアンスが SSO 認証要求を行う SSO サーバの URL を入力します。
- SSO サーバへの認証要求を暗号化するには、使用する秘密鍵を Secret Key に入力します。鍵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。最小文字数または最大文字数の制限はありません。秘密鍵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、セキュリティ アプライアンスと SiteMinder Policy Server の両方で設定します。
- Maximum Retries フィールドには、失敗した SSO 認証試行をセキュリティ アプライアンス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。
- Request Timeout フィールドには、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。

- HTTP Compression は、HTTP Compression の設定をデフォルト グループから継承するか、明示的に HTTP 圧縮を有効または無効にするかを指定します。特定のグループ ポリシーの SVC 接続で HTTP データの圧縮を有効または無効にするには、Inherit チェックボックスをクリアし、それぞれ Enable または Disable を選択します。デフォルトでは、SVC 圧縮は有効です。
- ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回線がアクティブであることを確認します。このメッセージの長さは変動します。Keepalive Ignore アトリビュートを使用して、セッション タイマーをアップデートするときに、指定したサイズ以下のすべてのメッセージをトラフィックではなくキープアライブ メッセージと見なすようセキュリティ アプライアンスに指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

- Deny Message アトリビュートは、WebVPN には正常にログインできたが VPN 権限がないリモート ユーザに配信するメッセージを次のように設定します。
  - Inherit チェックボックスを選択して、WebVPN には正常にログインできたが VPN 権限がないリモート ユーザに送信するメッセージをデフォルト グループから継承します。
  - Inherit チェックボックスをクリアし、フィールドのテキストを消去して、WebVPN には正常にログインできたが VPN 権限がないリモート ユーザにメッセージを送信しないようにします。
  - Inherit チェックボックスをクリアし、このフィールドで、WebVPN には正常にログインできたが VPN 権限がないリモート ユーザに送信するメッセージを作成または修正します。メッセージは 491 文字までの英数字で、特殊文字、スペース、句読点を使用できます。ただし、引用符は使用できません。復帰 / 改行は、2 文字としてカウントされます。テキストは、ログイン時に、リモート ユーザのブラウザに表示されます。デフォルトの拒否メッセージは、「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」です。

SSL VPN Client タブ アトリビュートの設定

SSL VPN Client（SVC）は、ネットワーク管理者が IPSec VPN クライアントをリモート コンピュータにインストールし、設定する必要なしに、リモート ユーザが IPSec VPN を利用できるようにする VPN トンネリング技術です。SVC は、すでにリモート コンピュータにある SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVC セッションを確立するには、リモート ユーザがブラウザにセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスを入力します。ブラウザがそのインターフェイスに接続し、WebVPN ログイン画面が表示されます。ユーザがログインと認証を終了し、セキュリティ アプライアンスがこのユーザを SVC が*必要な*ユーザとして識別した場合、セキュリティ アプライアンスはリモート コンピュータに SVC をダウンロードします。セキュリティ アプライアンスがこのユーザを SVC が*オプション*で使用できるユーザとして識別した場合、セキュリティ アプライアンスは SVC のインストールをスキップするリンクをユーザ画面に表示して、リモート コンピュータに SVC をダウンロードします。

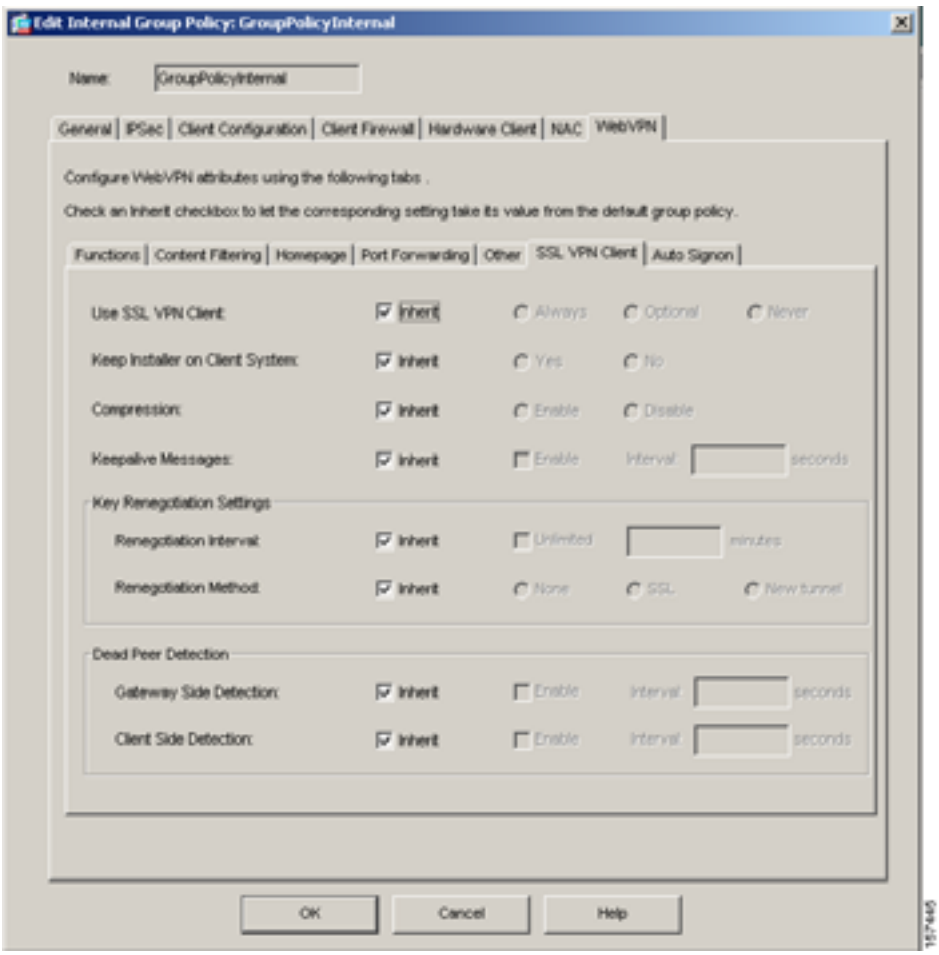
ダウンロード後、SVC は自己インストールおよび設定を行い、接続が終了したときに、（設定に応じて）リモート コンピュータに残るか、自己アンインストールします。

セキュリティ アプライアンスは、異なるリモート コンピュータのオペレーティング システム用に、複数の一意の SVC イメージをキャッシュ メモリに常駐させることができます。ユーザが接続しようとしたとき、セキュリティ アプライアンスは、イメージとオペレーティング システムが一致するまで、これらのイメージの一部を連続してダウンロードします。一致すると、SVC の全体をダウンロードします。リモート コンピュータのオペレーティング システムと最も一致する可能性が高いイメージが最初にダウンロードされるように SVC イメージを並べ替えて、接続セットアップ時間を最小にできます。SVC のインストールおよび使用の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の第 31 章「Configuring SSL VPN Client」を参照してください。

この設定ガイドの章の説明に従い、SVC を有効にした後、特定のグループに対して SVC を使用可能または必須にできます。この機能はデフォルトで無効になっています。SVC を使用可能または必須にする場合は、この項で説明するように、svc コマンドの連続を有効にできます。

Edit Internal Group Policy ウィンドウの WebVPN タブの SSL VPN タブ（図 2-42）を使用して、SSL VPN Client の接続の設定値を設定できます。各アトリビュートは、デフォルト グループ ポリシーから値を継承することも、Inherit チェックボックスをクリアして明示的に個別のアトリビュートを設定することもできます。

図 2-42　Edit Internal Group Policy の WebVPN タブの SSL VPN Client タブ



SSL VPN Client アトリビュートは、次のように設定します。

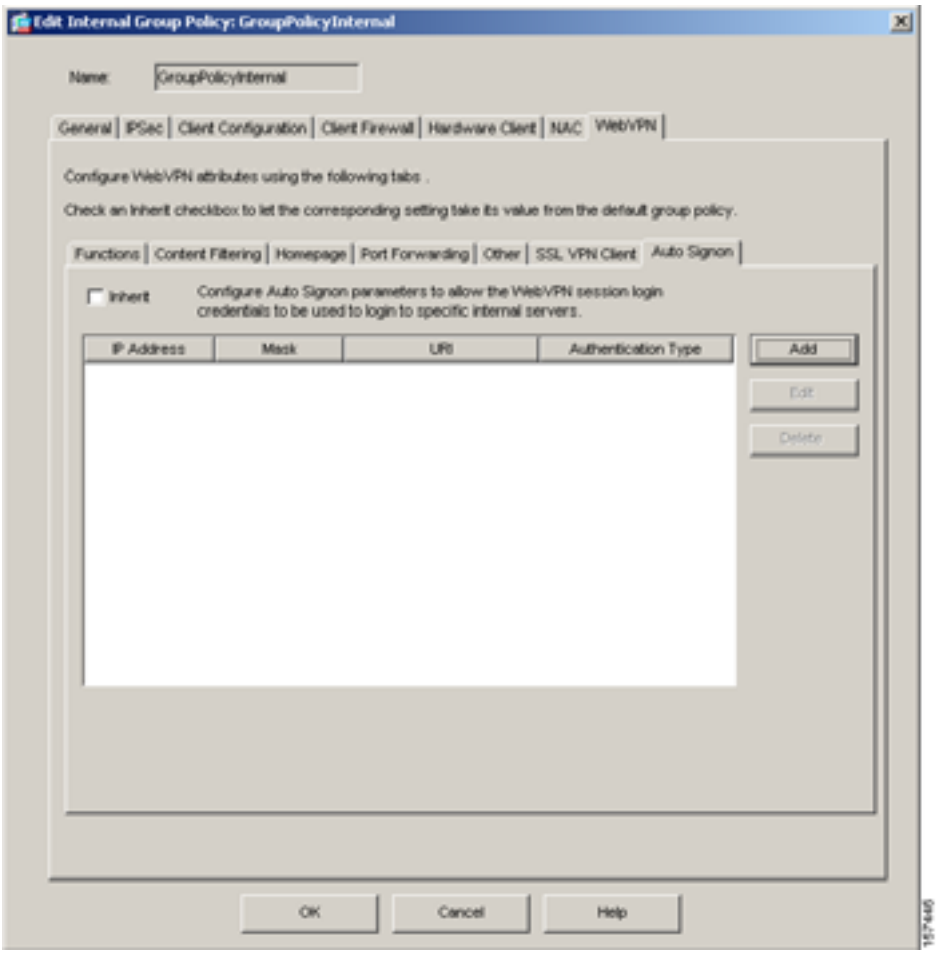
- Use SSL VPN Client の Inherit チェックボックスをクリアし、Always、Optional、または Never を選択して、いつ SSL VPN Client を使用するかを指定します。
- Keep Installer on Client System は、永続的な SVC インストールを有効にし、SVC の自動アンインストール機能を無効にします。**Yes** を選択すると、セキュリティ アプライアンスがリモート コンピュータに SVC ファイルをダウンロードし、SVC は後続の SVC 接続用にリモート コンピュータ上にインストールされたままとなり、リモート ユーザの SVC 接続時間を短縮できます。No を選択すると、セキュリティ アプライアンスは SVC ファイルをダウンロードしません。デフォルトでは、このアトリビュートは無効になっています。
- Compression は、SVC 接続での圧縮を有効または無効にします。SVC 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 SVC 間の通信パフォーマンスが向上します。
- Keepalive Messages アトリビュートは、キープアライブ メッセージの頻度を 15 ～ 600 秒の範囲で調整し、プロキシ、ファイアウォール、または NAT デバイスが接続のアイドル時間を制限する場合でも、これらのデバイスを経由する SVC 接続が開いたままになるようにします。Enable をクリックすると、Interval フィールドがアクティブになります。プロキシ、ファイアウォール、または NAT デバイスが接続のアイドル時間を制限する場合でも、これらのデバイスを経由する SVC 接続が開いたままになるように、キープアライブ メッセージの間隔（頻度）を調整できます。また、頻度を調整すると、リモート ユーザが Microsoft Outlook や Microsoft Internet Explorer などのソケットベース アプリケーションをアクティブに実行していない場合に、切断して再接続することがなくなります。

- Key Renegotiation Settings 領域のアトリビュートは、再ネゴシエーションの間隔と方式を定義します。セキュリティ アプライアンスと SVC が鍵の再生成を実行するとき、接続のセキュリティを高めるために、暗号鍵と初期ベクトルを再ネゴシエートします。
  - Renegotiation Interval は、セッション開始から鍵の再生成が実行されるまでの時間を分単位で指定します。指定できる値は Unlimited または 1 ～ 10080（1 週間）です。
  - Renegotiation Method は、SVC の鍵の再生成の際に SVC が新しいトンネルを確立するかどうかを指定します。None を選択すると、SVC の鍵の再生成が無効になります。SSL を選択すると、SVC の鍵の再生成の際に、SSL の再ネゴシエーションが実行されます。New tunnel を選択すると、SVC の鍵の再生成の際に、SVC が新しい VPN トンネルを作成します。
- Dead Peer Detection (DPD) 領域のアトリビュートは、セキュリティ アプライアンス（ゲートウェイ）または SVC が、ピアが応答しない状態、および接続が失敗した状態を早く検出できるようにします。この領域で選択したアトリビュートによって、接続のどちら側で DPD を実行するかが決まります。次のアトリビュートのどちらも、Inherit チェックボックスと Enable チェックボックスをクリアし、Interval フィールドをブランクのままにすると、そのアトリビュートが無効になります。
  - Gateway Side Detection は、セキュリティ アプライアンス（ゲートウェイ）による DPD 実行を有効にし、セキュリティ アプライアンスが DPD を実行する頻度を 30 ～ 3600 秒（1 時間）の範囲で指定します。disable を選択すると、セキュリティ アプライアンスによる DPD の実行が無効になります。
  - Client Side Detection は、SVC（クライアント）による DPD 実行を有効にし、SVC が DPD を実行する頻度を 30 ～ 3600 秒（1 時間）の範囲で指定します。

Auto Signon タブ アトリビュートの設定

WebVPN タブの Auto Signon タブ（図 2-43）を使用して、WebVPN ユーザの自動サインオンを設定または編集できます。

図 2-43　WebVPN の Auto Signon タブ

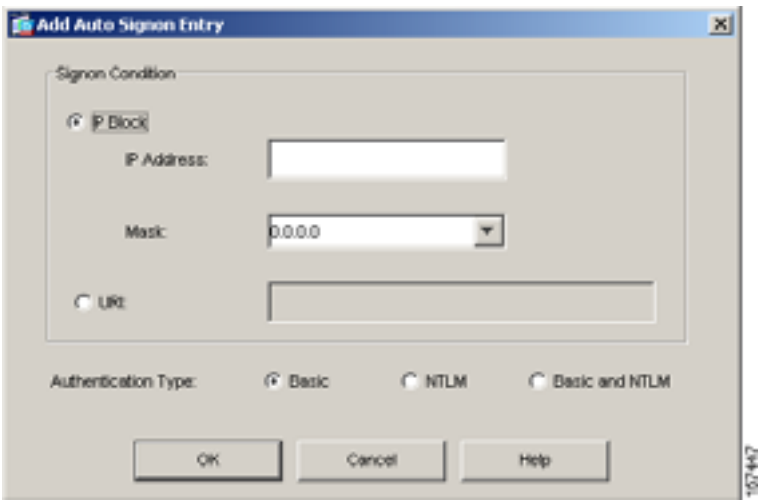


自動サインオンは、内部ネットワークに SSO 方式をまだ展開していない場合に使用できる簡素化された単一サインオン方式です。SSO は、Computer Associates の SiteMinder SSO サーバを使用してすでに展開しています。

Computer Associates の SiteMinder SSO サーバを使用して SSO を展開し、このソリューションをサポートするようにセキュリティ アプライアンスを設定することもできます。HTTP Forms プロトコルを用いる SSO を使用して、この方式をサポートするようにセキュリティ アプライアンスを設定できます。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、セキュリティ アプライアンスは、WebVPN ユーザがセキュリティ アプライアンスへのログインに使用したログイン クレデンシャルをこれら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、セキュリティ アプライアンスを設定します。セキュリティ アプライアンスが応答するように設定できる認証方式は、NTLM 認証、HTTP Basic 認証、またはこれらの両方です。

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。Auto Signon タブの Inherit チェックボックス以外のフィールドは、Add Auto Signon Entry または Edit Auto Signon Entry ダイアログボックス（図 2-44）と同じです。

図 2-44　Add Auto Signon Entry ダイアログボックス



エントリのフィールドを設定または修正するときは、次の説明に従ってください。

- Inherit：（Auto Signon タブのみ）このチェックボックスをクリアし、WebVPN ログイン クレデンシャルを使用して、特定の内部サーバにログインできるようにします。
- IP Address：次の Mask と組み合せて、認証されるサーバの IP アドレスの範囲を Add/Edit Auto Signon 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 と組み合せて、Add/Edit Auto Signon 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 Signon 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：認証タイプを Add/Edit Auto Signon ダイアログボックスで設定されたとおりに表示します（Basic HTTP、NTLM、または Basic and NTLM）。
- Add/Edit：（Auto Signon タブのみ）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。
- Delete：（Auto Signon タブのみ）クリックすると、Auto Signon テーブルで選択した自動サインオン命令が削除されます。

これで、内部グループ ポリシーの設定が完了しました。

CHAPTER 3

SVC の設定

SSL VPN Client（SVC）は、ネットワーク管理者がリモート コンピュータに IPSec VPN クライアントをインストールして設定しなくても、リモート ユーザが IPSec VPN クライアントの利点を活用できる VPN トンネリング テクノロジーです。SVC は、リモート コンピュータの既存の SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVC セッションを確立するには、リモート ユーザはセキュリティ アプライアンスの WebVPN 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。ブラウザはそのインターフェイスに接続して WebVPN のログイン ウィンドウを表示します。ユーザがログインと認証を完了し、ユーザが SVC を*必要としていること*をセキュリティ アプライアンスが確認すると、セキュリティ アプライアンスは SVC をリモート コンピュータにダウンロードします。セキュリティ アプライアンスが、SVC を使用する*オプション*がユーザにあると確認した場合、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをウィンドウに表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC は自身のインストールと設定を実行します。接続終了時に（設定に応じて）、SVC はリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

この項は、次の内容で構成されています。

SVC のインストール

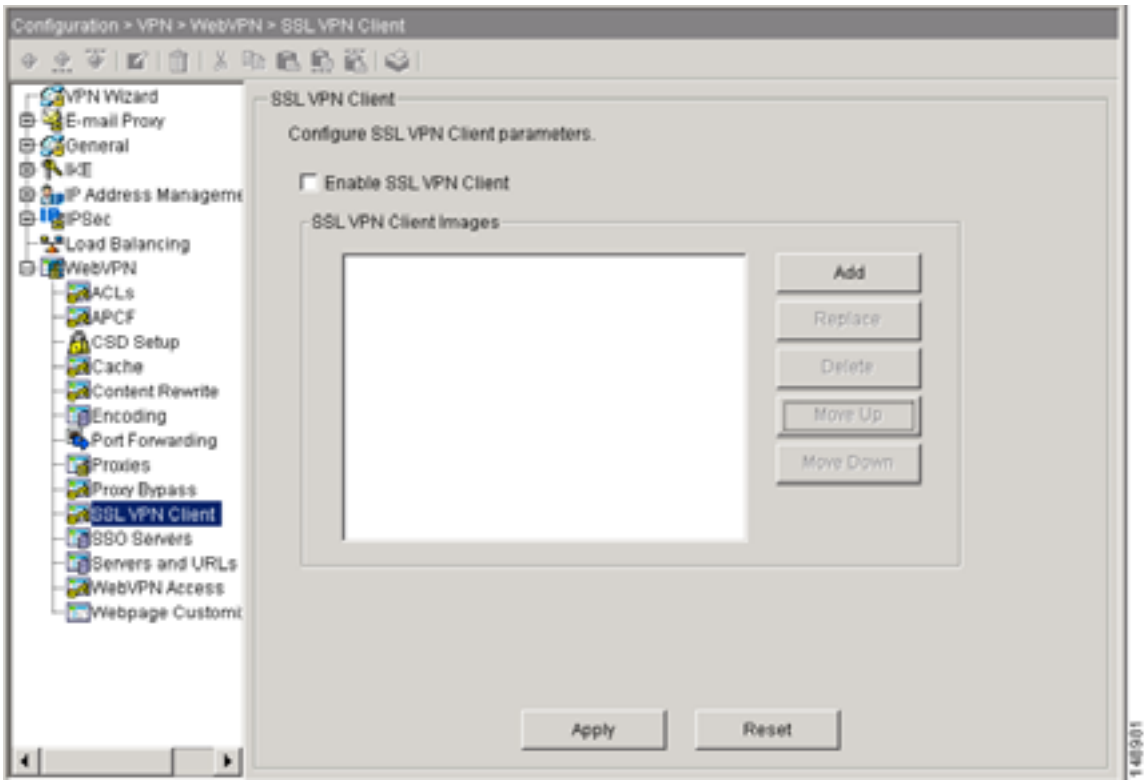
SVC のインストールは、SVC イメージをフラッシュ メモリにアップロードする手順、SVC イメージとして使用するフラッシュ メモリ上のファイルをセキュリティ アプライアンスに指定する手順、およびこのイメージをリモート コンピュータにダウンロードする順序を設定する手順で構成されています。

SVC をインストールするには、次の手順を実行します。

ステップ 1　SVC イメージをセキュリティ アプライアンスにアップロードします。ASDM ツールバーで、**Configuration** > **VPN** > **WebVPN** > **SSL VPN Client** を選択します。SSL VPN Client パネルが表示されます（図 3-1）。

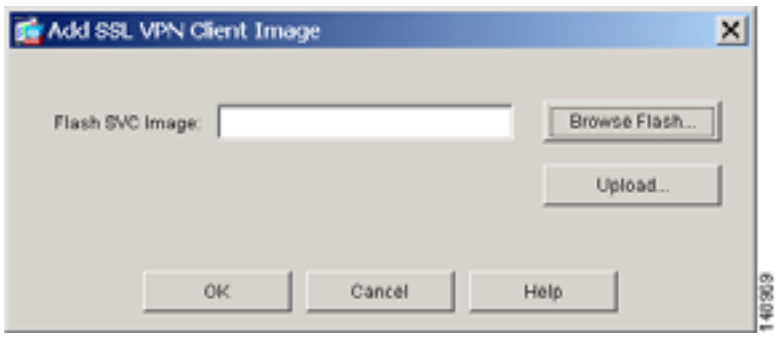
このウィンドウには、SVC イメージとして指定されているすべての SVC ファイルがリストされます。テーブルに表示される順序は、リモート コンピュータにダウンロードされる順序を反映しています。

図 3-1　SSL VPN Client ウィンドウ



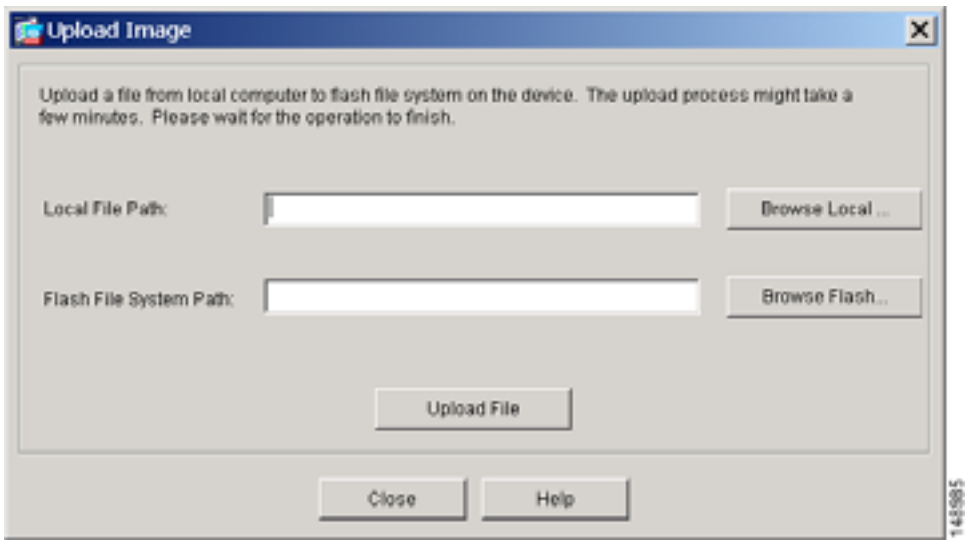
SVC イメージを追加するには、**Add** をクリックします。Add SSL VPN Client Image ダイアログボックスが表示されます（図 3-2）。

図 3-2　Add SSL VPN Client Image ダイアログ



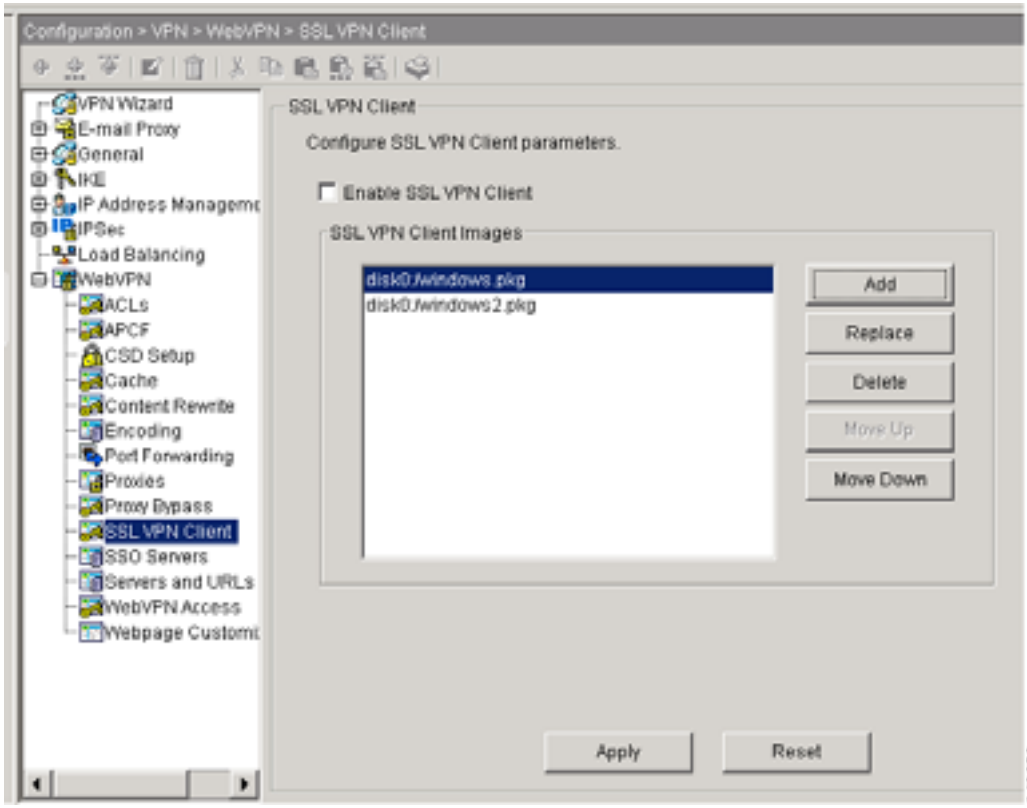
セキュリティ アプライアンスのフラッシュ メモリにすでにイメージがある場合は、Flash SVC Image フィールドにイメージの名前を入力して、**OK** をクリックします。それ以外の場合は、**Upload** をクリックして、ASDM を実行しているコンピュータを参照します。Upload Image ダイアログボックスが表示されます（図 3-3）。

図 3-3　Upload Image ダイアログ



Local File Path と Flash File System Path にパスを入力するか、パスを参照します。次に **Upload File** をクリックします。これで、SSL VPN Client ウィンドウに、指定した SVC イメージが表示されます（図 3-4）。

図 3-4　SVC イメージが表示された SSL VPN Client ウィンドウ

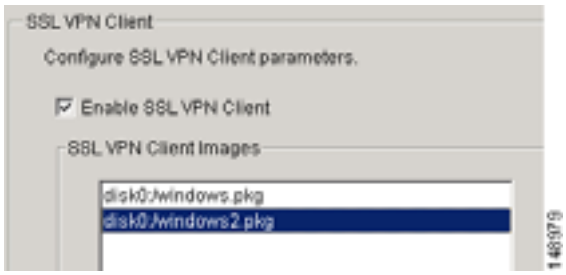


ステップ 2　イメージ名をクリックしてから、**Move Down** ボタンを使用して、リスト内のイメージの位置を変更します。

これにより、セキュリティ アプライアンスがリモート コンピュータにダウンロードする順序が設定されます。イメージ リストの一番上にある SVC イメージからダウンロードされます。このため、最も一般的なオペレーティング システムが使用するイメージをリストの一番上に移動する必要があります。

ステップ 3　**Enable SSL VPN Client** チェックボックスをオンにし、セキュリティ アプライアンスによる SVC イメージのダウンロードをイネーブルにします（図 3-5）。

図 3-5　Enable SSL VPN Client チェックボックス

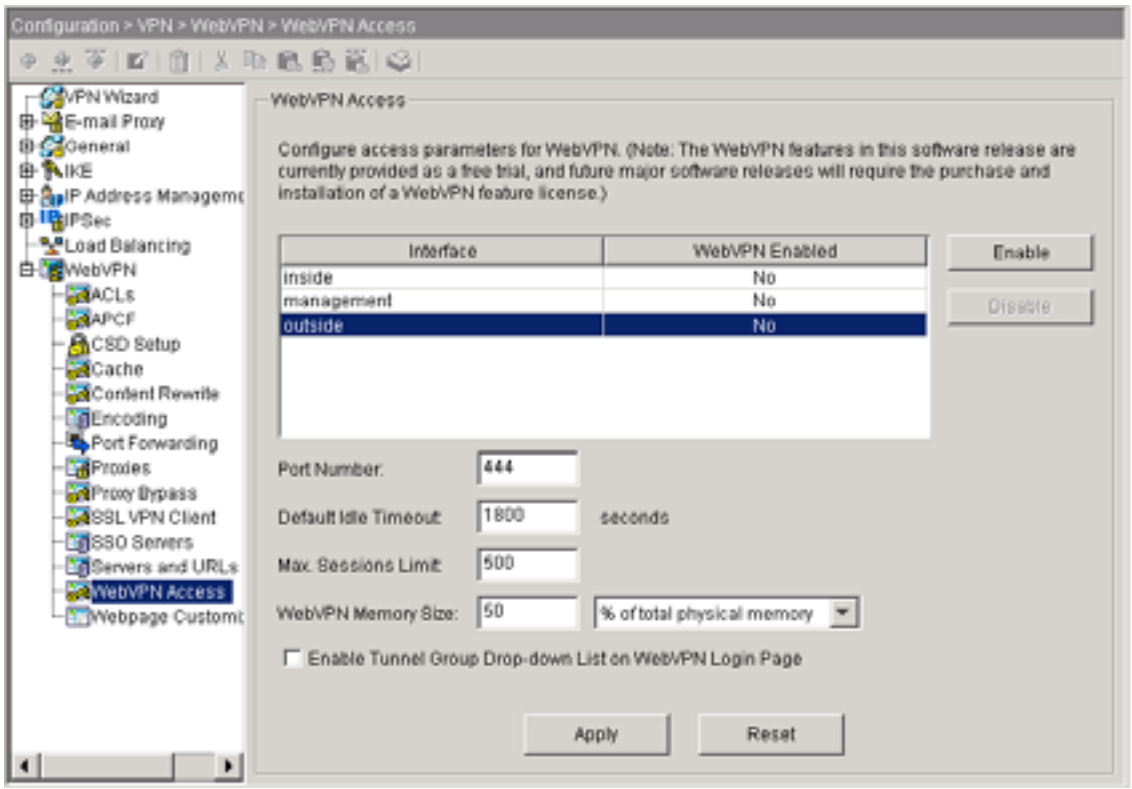


SVC の設定

SVC を設定するには、次の手順を実行します。

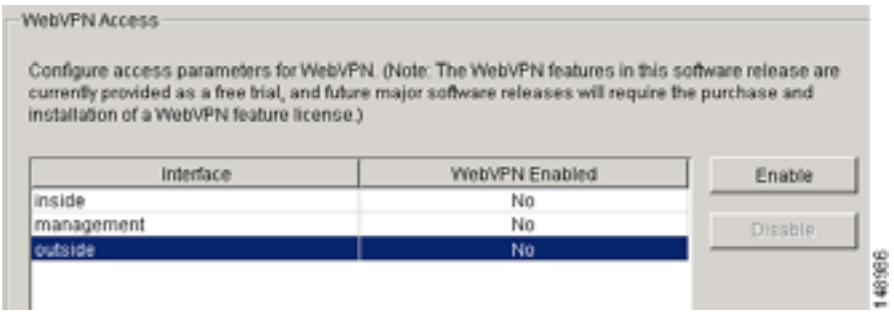
ステップ 1　インターフェイス上の WebVPN をイネーブルにします。ナビゲーション ペインから、**WebVPN Access** を選択します。WebVPN Access ウィンドウが表示されます（図 3-6）。

図 3-6　WebVPN Access ウィンドウ



インターフェイスを選択して、**Enable** をクリックします（図 3-7）。

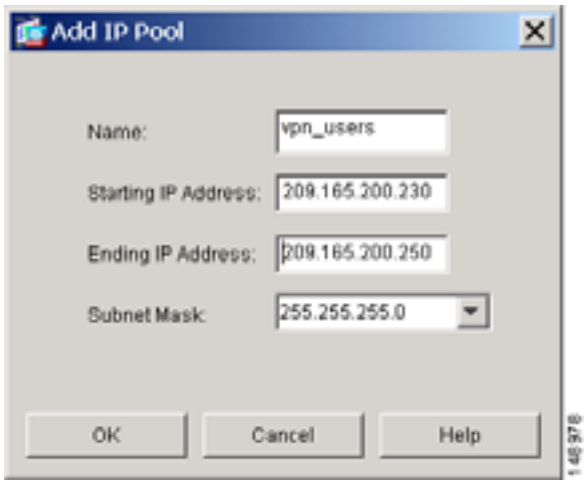
図 3-7　インターフェイスのイネーブル化



ステップ 2　アドレス割り当ての方式を設定します。DHCP とユーザ割り当てアドレッシングのいずれか 1 つ、または両方を使用できます。ローカル IP アドレス プールを作成して、プールをトンネル グループに割り当てることもできます。

IP アドレス プールを作成するには、**Configuration > VPN > IP Address Management > IP Pools** を選択します。**Add** をクリックします。Add IP Pool ダイアログが表示されます（図 3-8）。

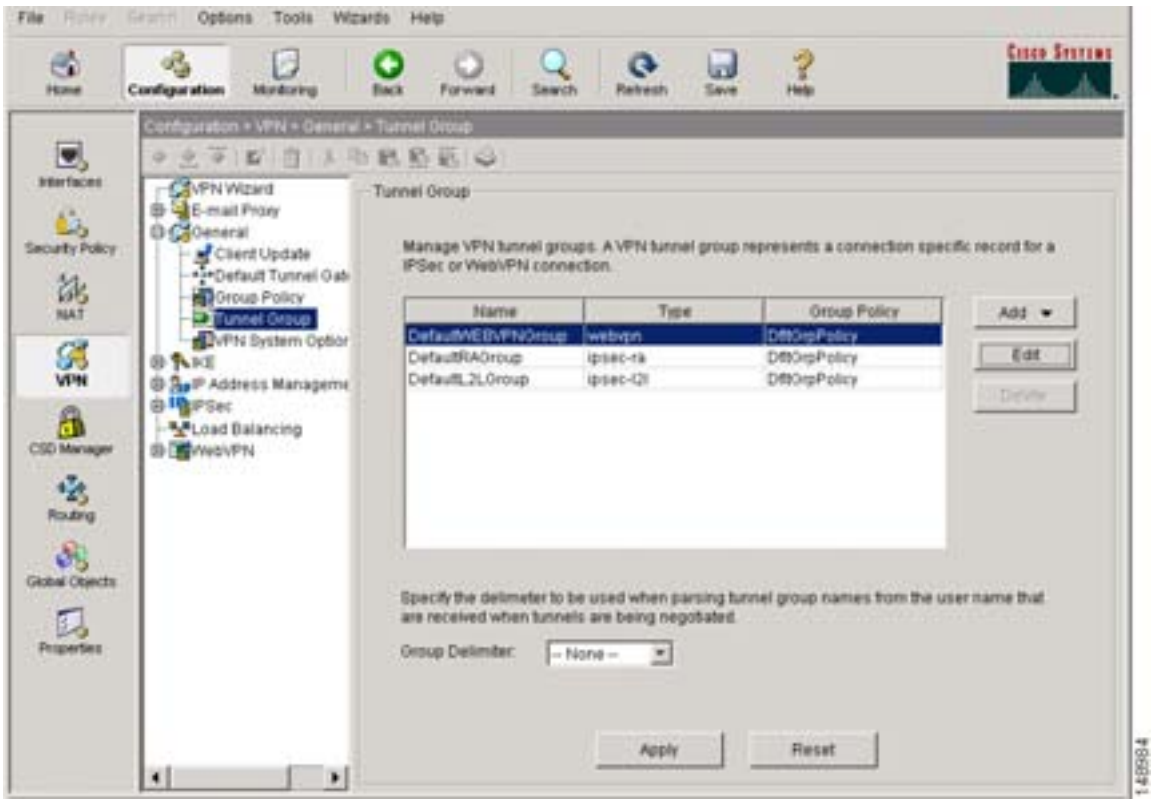
図 3-8　Add IP Pool ダイアログ



新しい IP アドレス プールの名前を入力します。開始 IP アドレスと終了 IP アドレスを入力してから、サブネット マスクを入力し、**OK** をクリックします。

ステップ 3　トンネル グループに IP アドレス プールを割り当てます。これを行うには、**Configuration > VPN > General > Tunnel Group** を選択します。Tunnel Group パネルが表示されます（図 3-9）。

図 3-9　Tunnel Group ウィンドウ



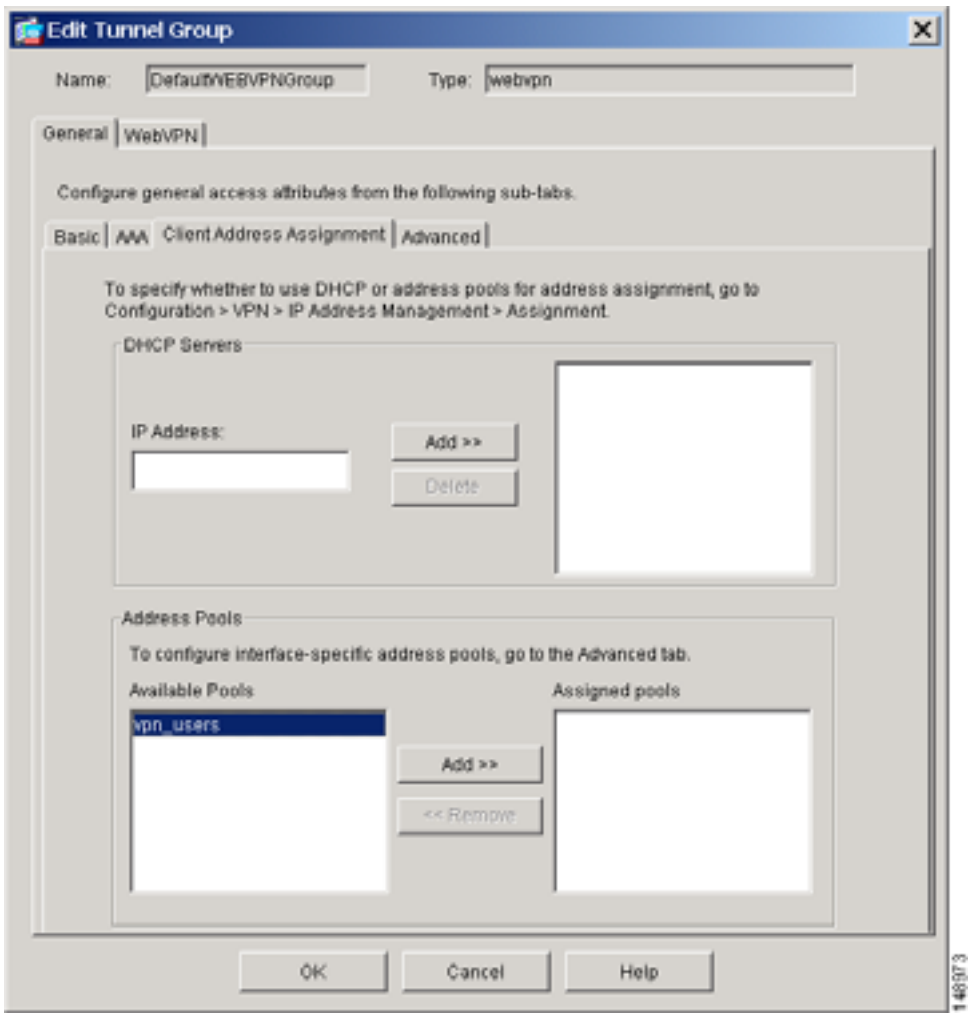
ステップ 4　テーブル内のトンネル グループを選択して、**Edit** をクリックします。

Edit Tunnel Group ダイアログが表示されます。

ステップ 5　**Client Address Assignment** タブをクリックします。

Address Pools グループ ボックスを含む **Client Address Assignment** タブが表示されます（図 3-10）。

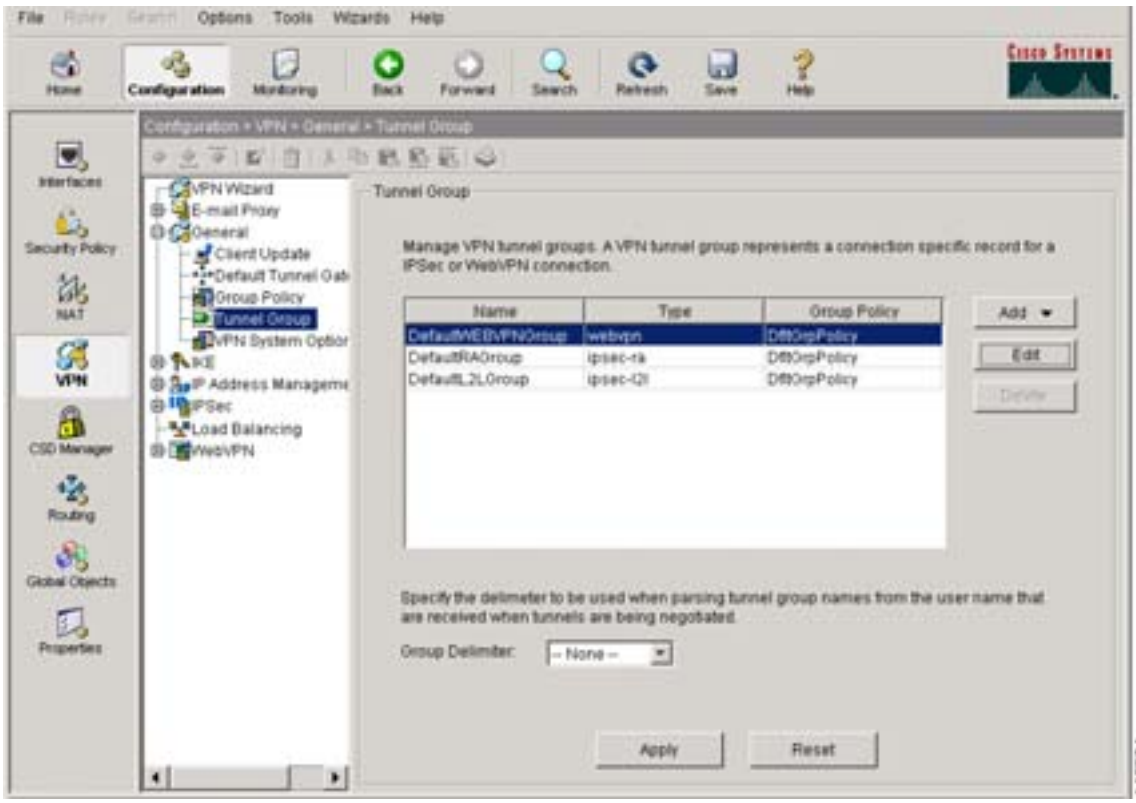
図 3-10　Edit Tunnel Group、General タブ、Client Address Assignment タブ



Address Pools グループ ボックスで、トンネル グループに割り当てるアドレス プールを選択して、**Add** をクリックします。

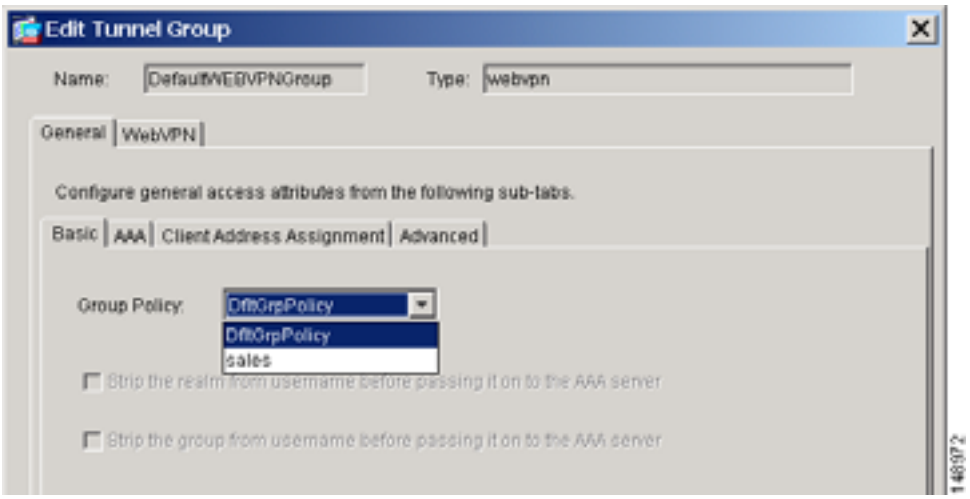
ステップ 6　トンネル グループにデフォルトのグループ ポリシーを割り当てます。**Configuration > VPN > General > Tunnel Group** を選択します。Tunnel Group ウィンドウが表示されます（図 3-11）。

図 3-11　Tunnel Group ウィンドウ



テーブルから WebVPN トンネル グループを選択して、**Edit** をクリックします。Edit Tunnel Group ダイアログ、**General** タブが表示されます（図 3-12）。

図 3-12　Edit Tunnel Group ダイアログ、General タブ、Basic タブ

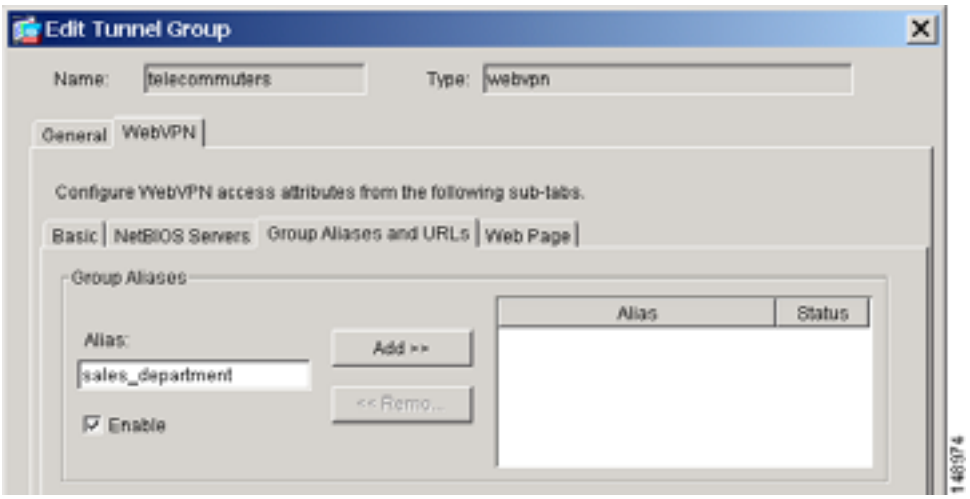


Group Policy リスト内のグループ ポリシーを選択して、**OK** をクリックします。

ステップ 7　WebVPN Login ページのグループ リストに表示されるグループ エイリアスを作成し、イネーブルにします。

WebVPN タブをクリックしてから、**Group Aliases and URLs** タブをクリックします。Group Aliases and URLs タブが表示されます（図 3-13）。

図 3-13　Edit Tunnel Group ダイアログ、WebVPN タブ、Group Aliases and URLs タブ



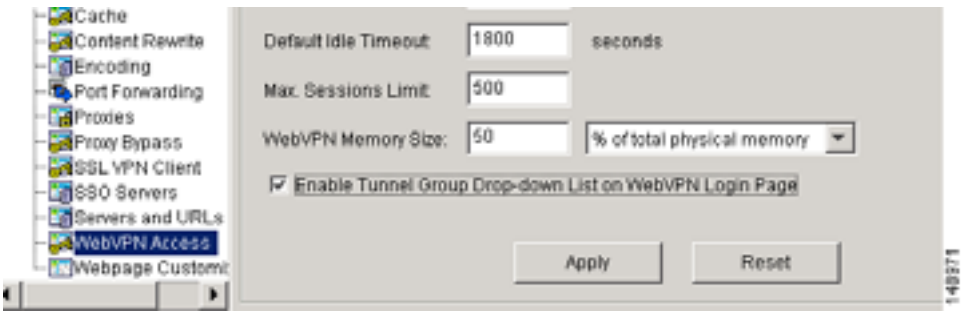
Alias フィールドに新しいエイリアスの名前を入力します。**Add** をクリックして、新しいエイリアスとして追加します。

Enable チェックボックスをオンにして、グループ エイリアスと URL をイネーブルにします。

ステップ 8　WebVPN Login ページ上のトンネルグループ リストの表示をイネーブルにします。

Configuration > VPN > WebVPN > WebVPN Access を選択します。WebVPN Access パネルが表示されます（図 3-14）。**Enable Tunnel Group Drop-Down List on WebVPN Login Page** チェックボックスをオンにして、**Apply** をクリックします。

図 3-14　WebVPN Access ウィンドウ、Enable Tunnel Group Drop-Down List on WebVPN Login Page チェックボックス

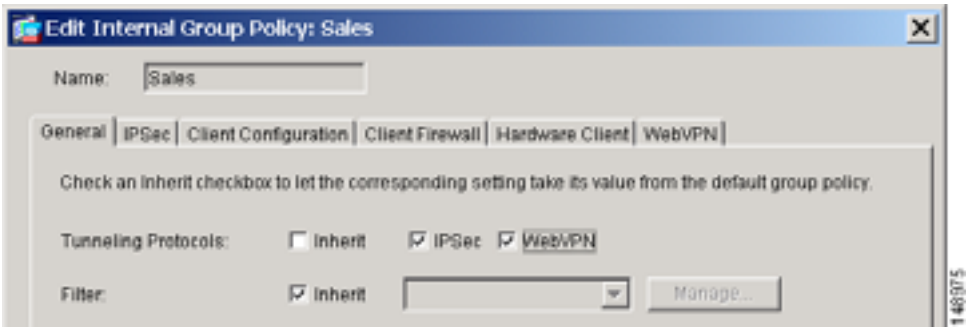


ステップ 9　グループまたはユーザで許可される VPN トンネリング プロトコルとして WebVPN を指定します。

ナビゲーション ペインから **Configuration > VPN > General > Group Policy** を選択します。Group Policy テーブル内のグループ ポリシーを選択して、**Edit** をクリックします。

Edit Internal Group Policy ダイアログの General タブが表示されます（図 3-15）。

図 3-15　Edit Internal Group Policy、General タブ



WebVPN チェックボックスをオンにして、トンネリング プロトコルとして WebVPN を追加します。

ステップ 10　ユーザまたはグループの SVC 機能を設定します。Edit User Accounts ダイアログと Edit Group Policy ダイアログの両方の **SSL VPN Client** タブにこれらの機能が表示されます。

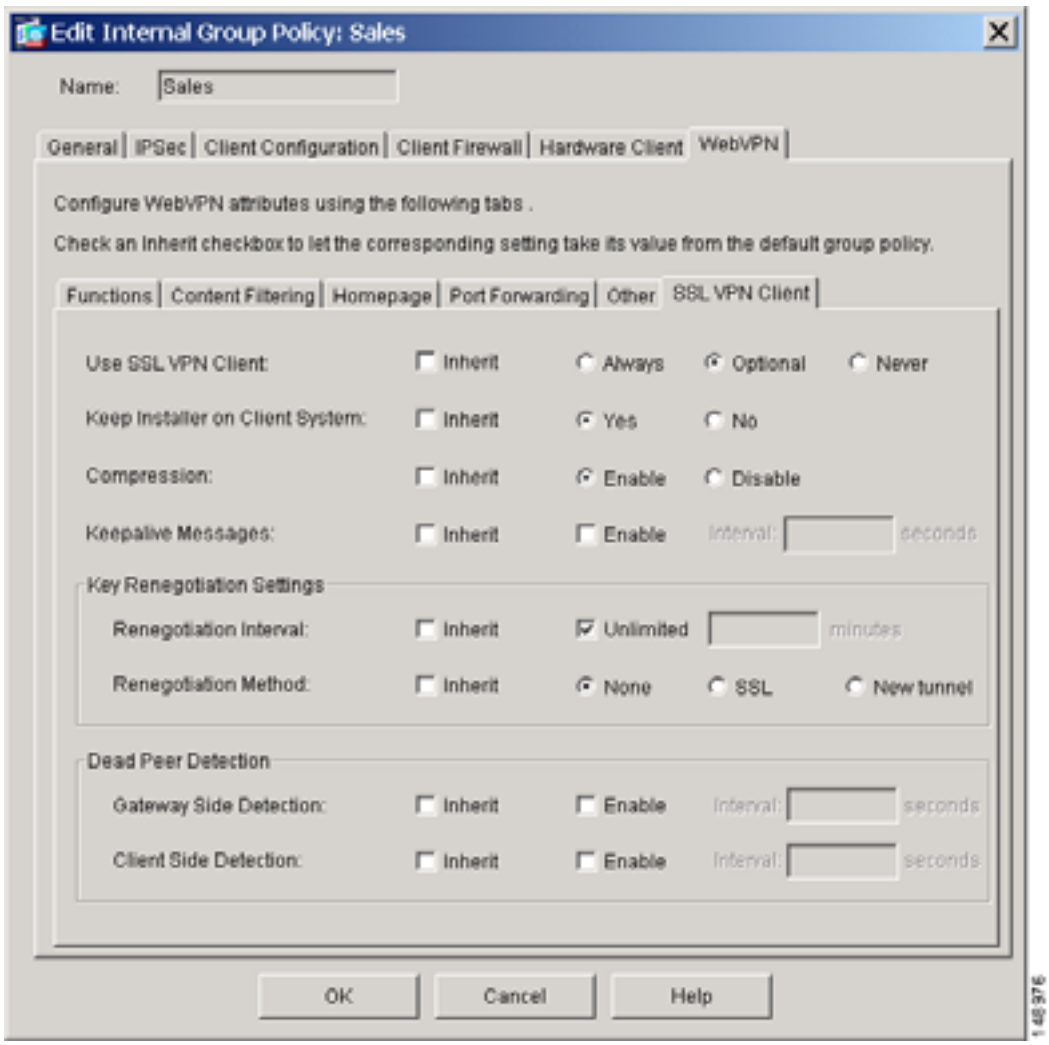
ユーザの **SSL VPN Client** タブを表示するには、次の手順を実行します。

- **Configuration > Properties > Device Administration > User Accounts** をクリックします。User Accounts パネルが表示されます。
- テーブル内のユーザを選択して、**Edit** をクリックします。Edit User Account ダイアログ、**General** タブが表示されます。
- **WebVPN** タブをクリックしてから、**SSL VPN** タブをクリックします。**SSL VPN Client** タブが表示されます（図 3-16）。

グループの **SSL VPN Client** タブを表示するには、次の手順を実行します。

- **Configuration > VPN > WebVPN > Group Policies** をクリックします。Group Policy パネルが表示されます。
- テーブル内のグループ ポリシーを選択して、**Edit** をクリックします。Edit Internal Group Policy ダイアログ、**General** タブが表示されます。
- **WebVPN** タブをクリックしてから、**SSL VPN** タブをクリックします。**SSL VPN Client** タブが表示されます。これは図 3-16 のユーザ アカウントで表示された **SSL VPN Client** タブと同じですが、こちらには **Inherit** チェックボックスが含まれていません。

図 3-16　SSL VPN Client タブ



(注)　ユーザ アカウントの場合、**SSL VPN Client** タブには、SVC 機能ごとにさらに **Inherit** チェックボックスが含まれます。**Inherit** チェックボックスをオンにすると、ユーザのグループ ポリシー内の設定に応じて機能が設定されます。

SSL VPN Client タブで次の機能を設定します。

Use SSL VPN Client：ユーザまたはグループで SVC を必須、オプション、またはディセーブルにします。

Keep Installer on Client System：リモート コンピュータの相手先固定 SVC のインストールをイネーブルにします。これにより、SVC の自動アンインストール機能がディセーブルになります。後続の SVC 接続では、SVC がリモート コンピュータにインストールされたままの状態になるため、リモート ユーザの SVC への接続時間が短縮されます。

Compression：SVC 圧縮は、転送されるパケットのサイズを減らすことによって、セキュリティ アプライアンスと SVC 間の通信パフォーマンスを向上させます。

Keepalive Messages：**Enable** チェックボックスをオンにし、キープアライブ メッセージの間隔をイネーブルにして調整し、接続のアイドル状態を維持できる時間がデバイスで制限される場合でも、プロキシ、ファイアウォール、または NAT デバイス経由の SVC 接続を開かれたままの状態にしておきます。

また、間隔を調整することによって、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベースのアプリケーションをアクティブに実行していないときに SVC が接続を解除して再接続しないようにすることができます。

seconds フィールドは、15 ～ 600 秒の範囲でメッセージの間隔を指定します。

Key Renegotiation Settings ：セキュリティ アプライアンスと SVC が鍵を再生成するときは、暗号鍵と初期ベクトルを再ネゴシエーションして接続のセキュリティを強化します。

- **Renegotiation Interval**：**Unlimited** チェックボックスをオフにして、セッションの開始から鍵の再生成までの分数を、1 ～ 10080（1 週間）で指定します。
- **Renegotiation Method**：**None** チェックボックスをオンにして鍵の再生成をディセーブルにしたり、**SSL** チェックボックスをオンにして鍵の再生成時の SSL 再ネゴシエーションを指定したり、**New tunnel** チェックボックスをオンにして SVC 鍵の再生成時に新しいトンネルを確立したりします。

Dead Peer Detection：Dead Peer Detection（DPD）は、ピアが応答していないために失敗した接続をセキュリティ アプライアンス（ゲートウェイ）または SVC で迅速に検出できるようにします。

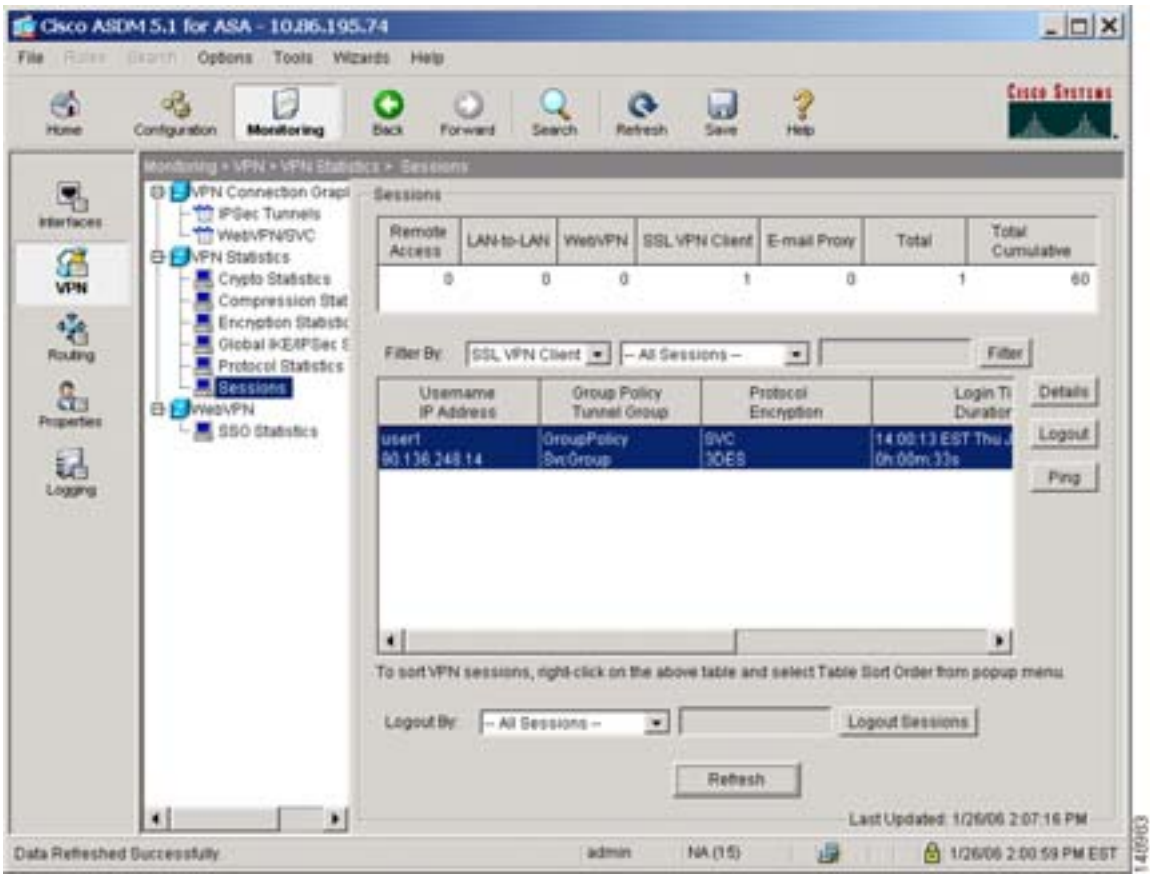
- **Gateway Side Detection**：**Enable** チェックボックスをオンにして、セキュリティ アプライアンス（ゲートウェイ）での DPD の実行を指定します。セキュリティ アプライアンスが DPD を実行する間隔を、30 ～ 3600 秒で入力します。
- **Client Side Detection**：**Enable** チェックボックスをオンにして、SVC（クライアント）での DPD の実行を指定します。SVC が DPD を実行する間隔を、30 ～ 3600 秒で入力します。

SVC セッションの表示

Sessions ウィンドウでアクティブな SVC セッションに関する情報を表示できます。

Monitoring > **VPN** > **VPN Statistics** > **Sessions** を選択します。Sessions ウィンドウが表示されます（図 3-17）。

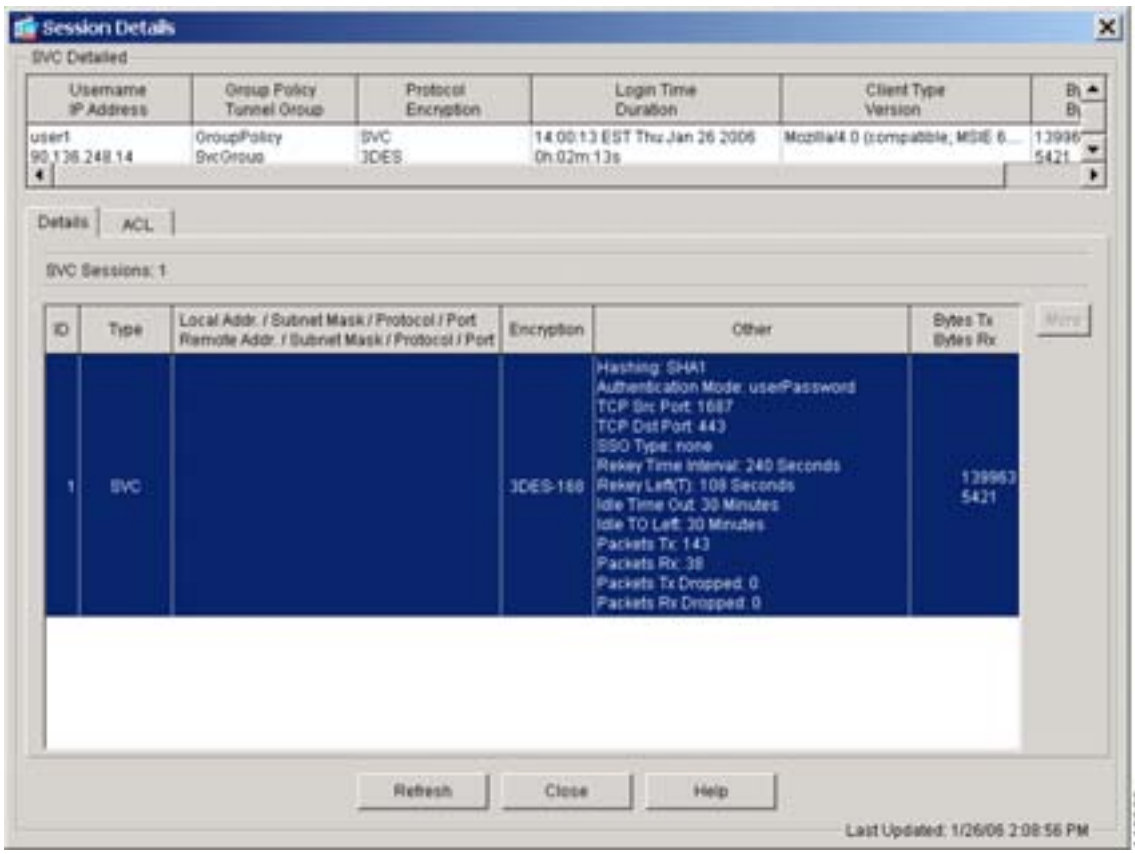
図 3-17　VPN Statistics Sessions ウィンドウ



Session Details ウィンドウでは、アクティブな SVC セッションに関する詳細情報を表示できます。

セッション テーブル内のセッションを選択して、**Details** をクリックします。Session Details ウィンドウが表示されます（図 3-18）。

図 3-18　Session Details ウィンドウ

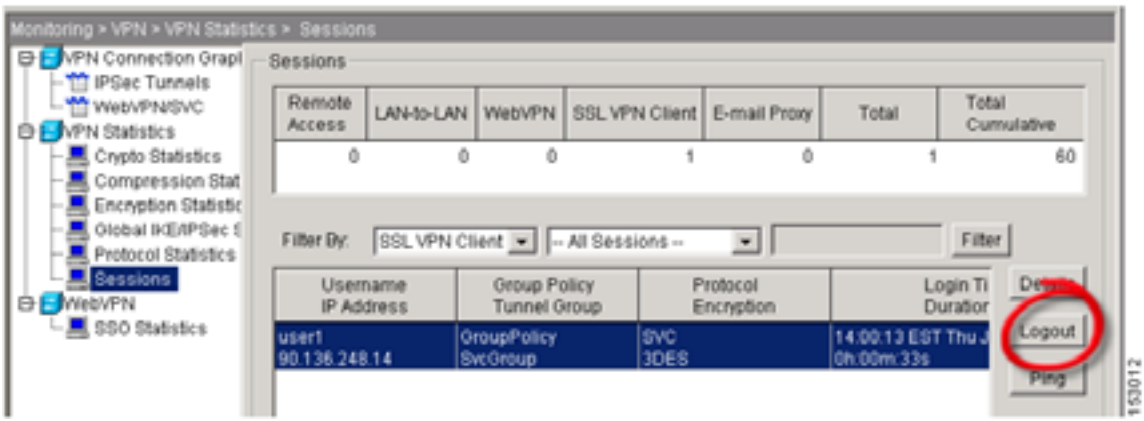


SVC セッションのログオフ

すべての SVC セッションをログオフするには、Session テーブルのアクティブ セッションのリストから終了するセッションを選択します。

Logout をクリックします。セッションが終了します。

図 3-19　セッションのログオフ



CHAPTER 4

Windows クライアントと VPN 3002 クライアントのクライアント アップデートの設定

ASDM には 2 種類のクライアント アップデートがあります。1 つ目はトンネル グループを介して Windows クライアントと VPN 3002 ハードウェア クライアントをサポートするクライアント アップデートで、2 つ目は自動アップデート サーバとして動作する ASA デバイスをサポートするクライアント アップデートです。この章では、Windows クライアントと VPN 3002 ハードウェア クライアントのトンネルグループ クライアント アップデート機能を設定する方法を説明します。

クライアント アップデート機能を使用すると、中心にいる管理者は、VPN クライアント ソフトウェアと VPN 3002 ハードウェア クライアント イメージを更新する時期を、VPN クライアント ユーザに自動的に通知できます。クライアントがリビジョン番号リストにあるソフトウェア バージョンをすでに実行している場合、ソフトウェアを更新する必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していない場合、更新する必要があります。この手順は、IPSec リモートアクセス トンネルグループのタイプだけに適用されます。

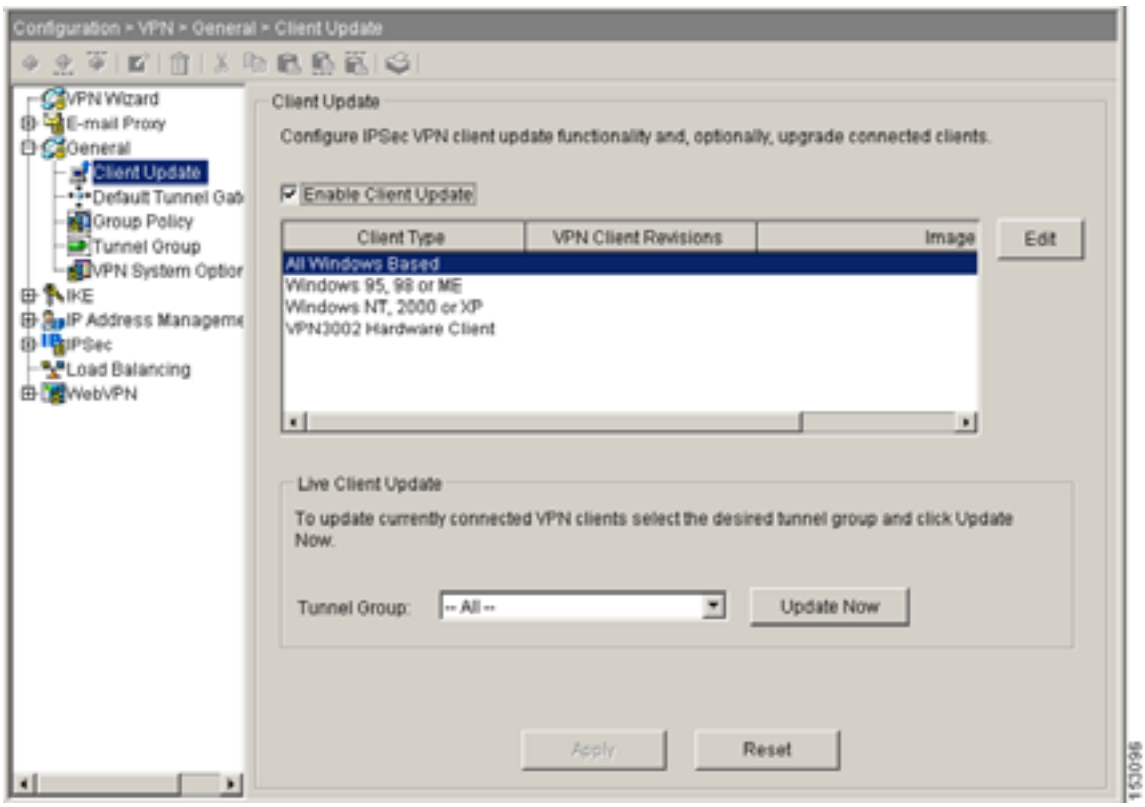
リモート ユーザは、旧式の VPN ソフトウェアまたはハードウェア クライアント バージョンを使用している可能性もあります。クライアント アップデートを実行すると、いつでも次の機能を行うことができます。

- クライアント リビジョンの更新をイネーブルにする
- アップデートを適用するクライアントのタイプとリビジョン番号を指定する
- アップデートを取得する URL または IP アドレスを提供する
- 必要に応じて、VPN クライアント バージョンを更新する必要があることを Windows クライアント ユーザに通知する
- Windows クライアントの場合、アップデートを実行するメカニズムをユーザに提供できる
- VPN 3002 ハードウェア クライアント ユーザの場合、アップデートは通知なしで自動的に行われる

クライアント アップデートを設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > General > Client Update** パスを選択して、Client Update ウィンドウに進みます。Client Update ウィンドウが開きます（図 4-1）。

図 4-1　Client Update ウィンドウ



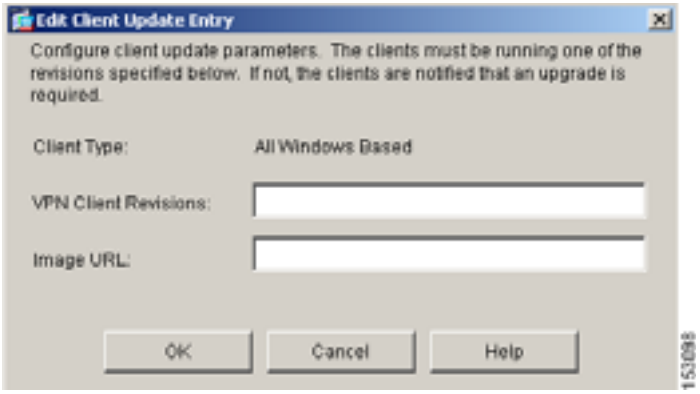
ステップ 2　Enable Client Update チェックボックスをオンにして、クライアント アップデートをイネーブルにします。

ステップ 3　クライアント アップデートを適用するクライアント タイプを選択します。使用可能なクライアント タイプは、All Windows-Based、Windows 95, 98 or ME、Windows NT 4.0, 2000 or XP、および VPN 3002 Hardware Client です。

クライアントがリビジョン番号リストにあるソフトウェア バージョンをすでに実行している場合、ソフトウェアを更新する必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していない場合は、更新する必要があります。最大 3 つのクライアント アップデート エントリを指定できます。All Windows Based は、許容されるすべての Windows プラットフォームを網羅します。これを選択する場合、個々の Windows クライアント タイプは指定しないでください。

ステップ 4　許可されるクライアント　リビジョンおよび更新されたソフトウェアのソースまたはクライアント アップデートのファームウェア イメージを指定するには、Edit をクリックします。選択したクライアント タイプを示した Edit Client Update Entry ウィンドウ（図 4-2）が表示されます。

図 4-2　Edit Client Update Entry ウィンドウ



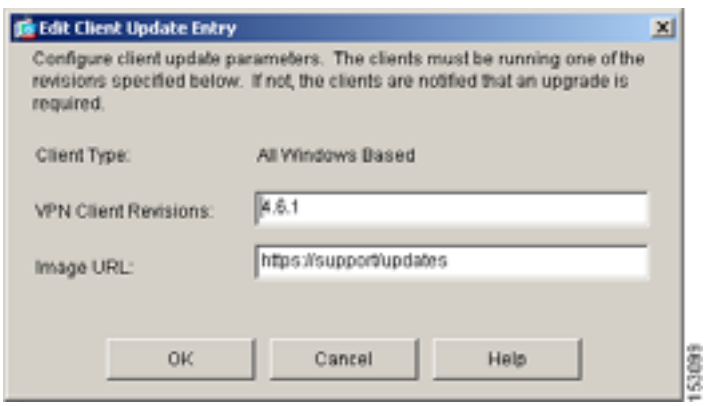
ステップ 5　セキュリティ アプライアンス全体にわたって、選択したタイプのすべてのクライアントに適用するクライアント アップデートを指定します。つまり、クライアント タイプ、更新されたイメージを取得する URL または IP アドレス、およびそのクライアントの許可されるリビジョン番号を指定します。リビジョン番号は、カンマで区切って最大 4 つまで指定できます。OK をクリックした後に、該当するカラム（Client Upgrade ウィンドウのテーブル）にエントリが表示されます。

ユーザのクライアント リビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合は、クライアントを更新する必要はありません。

（注）　すべての Windows クライアントでは、URL のプレフィクスとしてプロトコル http:// または https:// を使用する必要があります。VPN 3002 ハードウェア クライアントの場合は、代わりにプロトコル tftp:// を指定する必要があります。

図 4-3 に、4.6.1 より前のリビジョンを実行しているリモートアクセス トンネルグループのすべての Windows クライアントでクライアント アップデートを開始し、アップデートを取得する URL（https://support/updates）を指定する例を示します。

図 4-3　Edit Client Update Entry の例



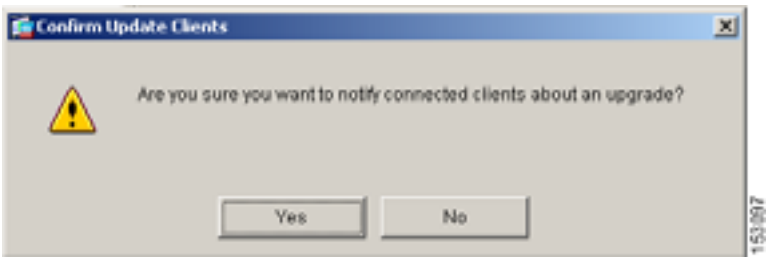
または、すべての Windows クライアントではなく、個々のクライアント タイプ専用にクライアント アップデートを設定することもできます（ステップ 3 を参照）。

VPN 3002 クライアントは、ユーザの介入なしに更新されるため、ユーザは通知メッセージを受け取りません。

たとえば **`https://support/updates/vpnclient.exe`** のように、URL の最後にアプリケーション名を含めると、ブラウザが自動的にアプリケーションを起動します。

ステップ 6　必要に応じて、クライアントのアップデートが必要な、最新の状態でない Windows クライアントを持つアクティブなユーザに通知を送信できます。この通知を送信するには、Client Update ウィンドウの Live Client Update 領域を使用します。トンネル グループを選択し（または All を選択）、Update Now をクリックします。接続中のクライアントにアップグレードを通知するかどうかを確認するダイアログボックス（図 4-4）が表示されます。

図 4-4　Confirm Update Clients ダイアログボックス



これらのユーザにはポップアップ ウィンドウが表示され、ブラウザを起動して URL に指定したサイトから更新されたソフトウェアをダウンロードすることができます。このメッセージのうち設定できる部分は URL だけです（ステップ 4 または 5 を参照）。アクティブでないユーザは、次にログインしたときに通知メッセージを受け取ります。この通知は、すべてのトンネル グループのすべてのアクティブなクライアントに送信するか、または特定のトンネルグループのクライアントに送信することができます。

ユーザのクライアント リビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合、クライアントを更新する必要はなく、通知メッセージはユーザに送信されません。VPN 3002 クライアントは、ユーザの介入なしに更新されるため、ユーザは通知メッセージを受け取りません。

CHAPTER 5

DDNS アップデートの設定

この章では、Dynamic DNS（DDNS; ダイナミック DNS）アップデートを設定する方法、つまり、最新の IP アドレスとホスト名の情報で 2 種類の DNS Resource Record（RR）を更新するプロセスを説明します。この 2 種類のレコードを更新するシナリオは複数存在しますが、この章では、次の一般的なシナリオを設定する手順を示します。

DHCP クライアントは、DHCP サーバに両方の DNS RR の更新を要求します。PTR RR だけを更新するように設定されたサーバは、クライアントの要求を受け入れ、A RR と PTR RR の両方を更新します。

この章には、次の項があります。

DDNS RR の概要

DDNS は、アドレスとドメイン名とのマッピングを提供し、DHCP 割り当て IP アドレスが頻繁に変更される場合でもホストが互いを発見できるようにします。マッピングは、DNS サーバに常駐する 2 種類のレコードに含まれます。これらのレコードは A RR と PTR RR です。このレコードを使用すると、IP アドレスまたはドメイン名のどちらかでホストを特定できます。A RR にはドメイン名から IP アドレスへのマッピングが含まれ、PTR RR には IP アドレスからドメイン名へのマッピングが含まれます。これらのレコードで DDNS アップデートを実行する 2 つの方式（RFC 2136 で定義された IETF 標準および汎用 HTTP 方式）のうち、セキュリティ アプライアンスは今回のリリースで IETF 方式をサポートしています。

アップデートをどのように設定するかに応じて、各レコードを DHCP サーバまたはクライアントのどちらかで更新できます。クライアントは、代行してアップデートを実行するようにサーバに要求できます。ただし、サーバでは、クライアントの要求を受け入れるか、無効にするかを設定する必要があります。

PTR RR を更新するには、DHCP サーバがクライアントの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を認識する必要があります。クライアントは、Client FQDN と呼ばれる DHCP オプションを使用してサーバに FQDN を提供します。

この章では、A RR と PTR RR の両方を更新するように DHCP サーバを設定する手順を示します。これは、最も一般的な設定の 1 つです。『*Cisco Security Appliance Command Line Configuration Guide*』に記載されている他の設定シナリオは、次のとおりです。

- DHCP クライアントがスタティック IP アドレスの A RR と PTR RR の両方を更新します。
- DHCP クライアントが A RR と PTR RR の両方を更新します。DHCP サーバは、クライアントアップデートの要求を受け入れます。設定を通じて FQDN が提供されます。
- DHCP クライアントに、どちらの RR も更新しないようにサーバに指示する FQDN オプションが組み込まれます。サーバはクライアントの要求を無効にし、両方の RR を更新します。
- DHCP クライアントが A RR を更新し、DHCP サーバが PTR レコードを更新します。クライアントはサーバからのドメイン名を使用して、FQDN を形成します。

DDNS 例の概要：サーバが両方のレコードを更新する場合

この項では、デフォルトで PTR RR アップデートだけを実行するように DHCP サーバを設定します。ただし、サーバは A アップデートと PTR アップデートの両方を実行するというクライアントの要求を受け入れます。

この設定例を実行するには、次のタスクを実行します。

1. DDNS アップデート方式を定義します。
2. DDNS アップデート方式をセキュリティ アプライアンス インターフェイスに割り当てます。
3. DHCP サーバを設定します。

(注)　この手順を行う前に、DHCP サーバと DNS クライアントを設定し、インターフェイス上で DHCP をイネーブルにしていることを前提とします。

アップデート方式の定義

DDNS のアップデート方式を設定するには、次の手順を実行します。

ステップ 1　**Configuration** > **Properties** > **DNS** > **Dynamic DNS** ウィンドウで、**Add** をクリックします。

図 5-1 のように、Edit Dynamic DNS Update Methods ダイアログボックスが表示されます。

図 5-1　Edit Dynamic DNS Update Methods ダイアログボックス

ステップ 2　Name フィールドに、DDNS 方式の名前を入力します。

この例では、方式に ddns-3 という名前が付いています。

ステップ 3　Days フィールドに、アップデートを行う間隔（日数）を入力します。

日数の範囲は、0 ～ 364 です。

ステップ 4　Hours メニューから、アップデートを行う間隔（時間数）を選択します。

ステップ 5　Minutes メニューから、アップデートを行う間隔（分数）を選択します。

この例では、毎分アップデートを行うようにスケジューリングします。

ステップ 6　Seconds メニューから、アップデートを行う間隔（秒数）を選択します。

（注）　この時間単位は、追加式です。つまり、日数に 0、時間数に 0、分数に 5、秒数に 15 を入力した場合、このアップデート方式がアクティブである限り、5 分 15 秒ごとにアップデートが行われます。

ステップ 7　Update Records の隣で、**Both (PTR and A Records)** オプション ボタンまたは **A Records only** オプション ボタンをクリックして、レコードを更新するように DHCP クライアントを設定します。

（注）　この方式の設定を無効にするようにインターフェイスまたは DHCP サーバを設定できるため、いずれかのオプション ボタンを選択できます。

ステップ 8　**OK** をクリックして、アップデート方式の設定を受け入れます。

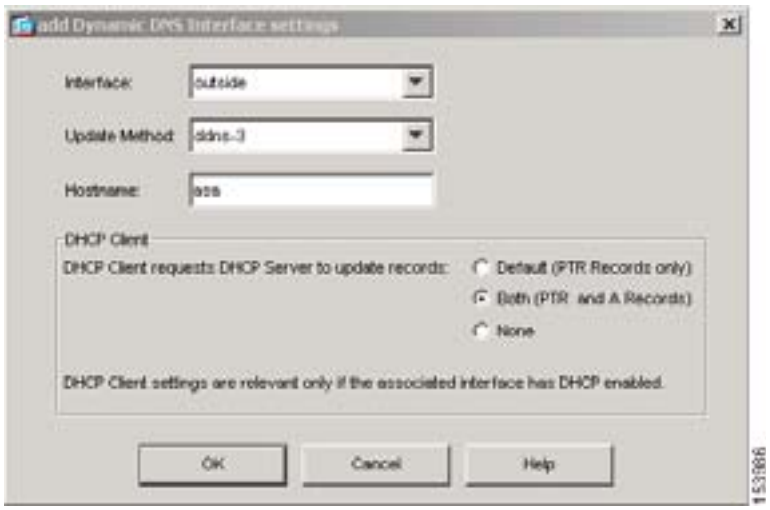
インターフェイスへのアップデート方式の割り当て

DDNS のアップデート方式をセキュリティ アプライアンス インターフェイスに設定するには、次の手順を実行します。

ステップ 1　**Configuration** > **Properties** > **DNS** > **Dynamic DNS** ウィンドウで、**Add** をクリックします。

図 5-2 のように、Add Dynamic DNS Interface Settings ダイアログボックスが表示されます。

図 5-2　Add Dynamic DNS Interface Settings ダイアログボックス



ステップ 2　Interface メニューから、設定するインターフェイスを選択します。

この例では、outside インターフェイスを選択します。

ステップ 3　Update Method メニューから、インターフェイスに適用するアップデート方式を選択します。

この例では、ddns-3 を選択しています。

ステップ 4　Hostname フィールドに、DDNS のホスト名を入力します。

この例では、asa を入力しています。

ステップ 5　DHCP Client 領域で、**Both (PTR and A Records)** をクリックします。

ステップ 6　**OK** をクリックして、インターフェイスの設定を受け入れます。

Add Dynamic DNS Interface Settings ダイアログボックスが閉じます。

ステップ 7　Dynamic DNS パネルの一番下で、Both (PTR Records and A Records) をクリックして、両方の RR を更新するようにグローバル DHCP サーバのアップデート設定を設定します。

ステップ 8　Apply をクリックして、新しい DDNS の設定をセキュリティ アプライアンスの実行コンフィギュレーションに追加します。

DHCP サーバの設定

DHCP サーバが PTR レコードを更新し、さらに DHCP クライアントのアップデート要求を受け入れるように設定するには、次の手順を実行します。

ステップ 1　**Configuration** > **Properties** > **DHCP Services** > **DHCP Server** ウィンドウで、DNS レコードを更新する DHCP サーバを選択します。

ステップ 2　Dynamic DNS Settings for DHCP Server 領域で、次の手順を実行します。

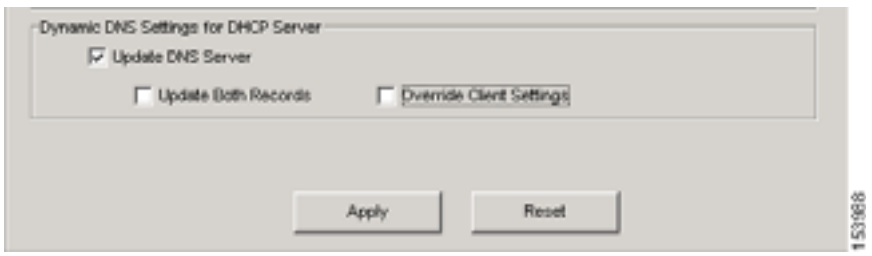
a. **Update DNS Clients** チェックボックスをオンにします。

b. **Update Both Records** チェックボックスをオフにします。

c. **Override Client Settings** チェックボックスをオフにします。

図 5-3 のように、Dynamic DNS Settings for DHCP Server 領域が表示されます。

図 5-3　Dynamic DNS Settings for DHCP Server 領域



ステップ 3　**Apply** をクリックして、DHCP サーバの設定をセキュリティ アプライアンスの実行コンフィギュレーションに追加します。

CHAPTER 6

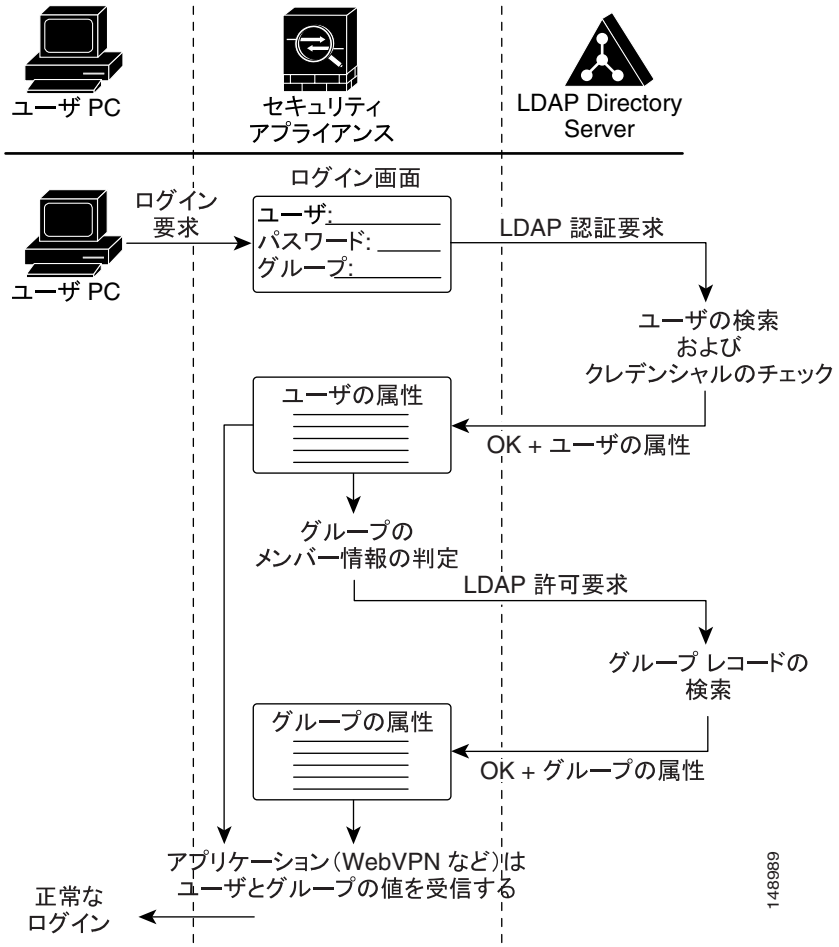
LDAP AAA サーバの設定

この章では、セキュリティ アプライアンスと同じ内部ネットワーク上にある Microsoft Active Directory Server（LDAP）を使用して、セキュリティ アプライアンスのユーザ認証と許可を設定する設定例を示します。この章には、次の項があります。

LDAP トランザクションの概要

図 6-1 に、LDAP ディレクトリ サーバを使用したセキュリティ アプライアンスのユーザ認証と許可の主なトランザクションを示します。

図 6-1　LDAP 認証と許可のトランザクション フロー



LDAP アトリビュート マップの作成

LDAP 認証と許可用にセキュリティ アプライアンスを設定するには、まずカスタマー定義のアトリビュート名をシスコの LDAP アトリビュート名にマッピングする LDAP アトリビュート マップを作成する必要があります。これにより、セキュリティ アプライアンスが認識するシスコ名を使用して、既存のアトリビュート名を変更する必要がなくなります。

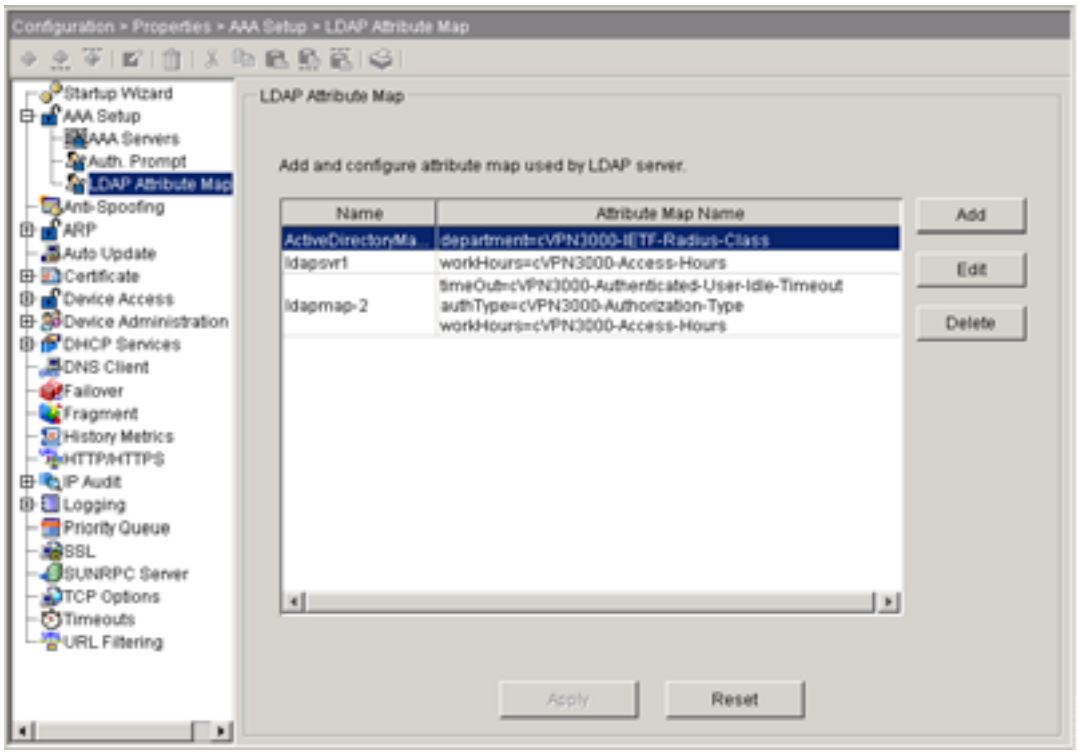
（注） アトリビュート マッピング機能を適切に使用するには、シスコの LDAP アトリビュートの名前と値およびユーザ定義のアトリビュートの名前と値を理解する必要があります。シスコの LDAP アトリビュートのリストについては、『*Cisco Security Appliance Command Line Configuration Guide*』の付録「Configuring an External Server for Authorization and Authentication」を参照してください。

新しい LDAP アトリビュート マップを作成するには、次の手順を実行します。

ステップ 1　Cisco ASDM ウィンドウで、**Configuration > Properties > AAA Setup > LDAP Attribute Map** を選択します。

図 6-2 のように、ウィンドウの右側に LDAP Attribute Map 領域が表示されます。

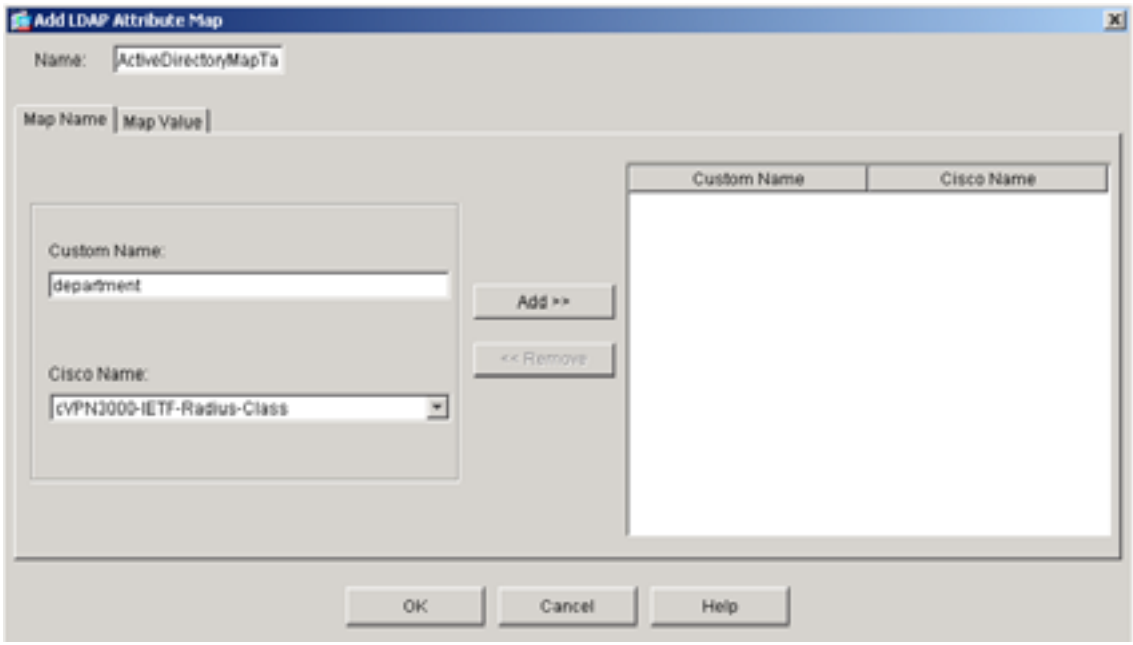
図 6-2　LDAP Attribute Map 領域



ステップ 2　LDAP Attribute Map 領域で、**Add** をクリックします。

図 6-3 のように、Add LDAP Attribute Map ダイアログボックスが表示されます。

図 6-3　Map Name タブが選択された Add LDAP Attribute Map ダイアログボックス



ステップ 3　タブの上にある Name フィールドに、LDAP アトリビュート マップの名前を入力します。

この例では、アトリビュート マップに ActiveDirectoryMapTable という名前を付けます。

ステップ 4　Map Name タブが選択されていない場合は、ここで選択します。

ステップ 5　Map Name タブの Custom Name（ユーザ定義のアトリビュート名）フィールドに、シスコのアトリビュート名にマッピングするアトリビュートの名前を入力します。

この例では、カスタム名は *department* です。

ステップ 6　Cisco Name メニューからシスコ名を選択します。カスタム名は、このシスコ名にマッピングされます。

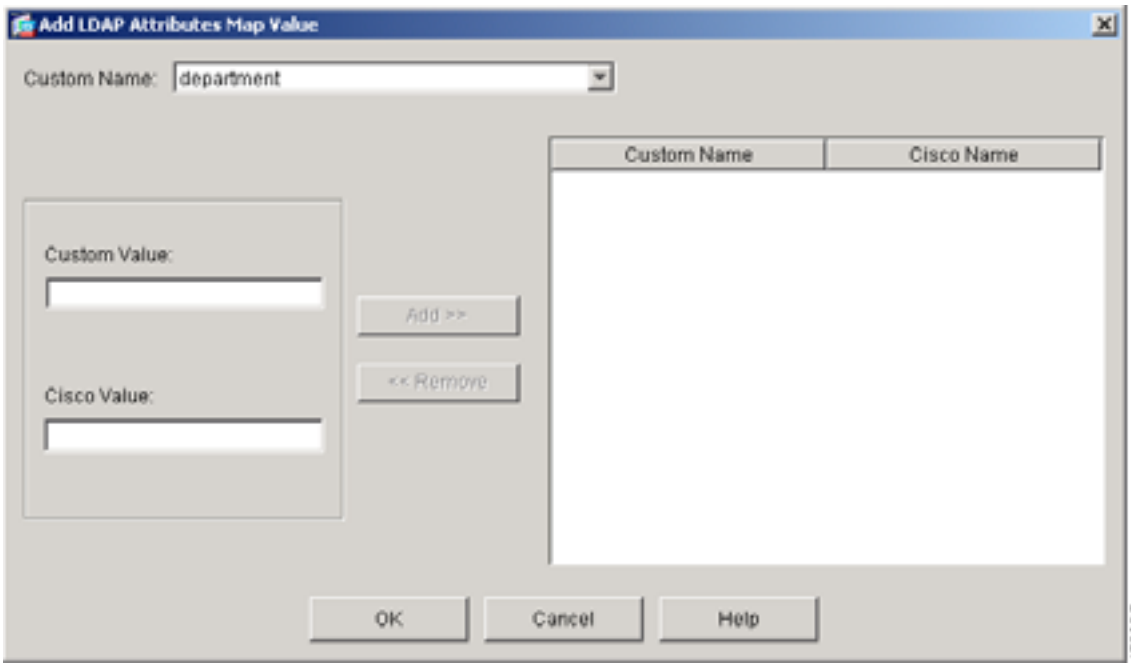
この例では、シスコ名は cVPN3000-IETF-Radius-Class です。図 6-1 のように、セキュリティ アプライアンスはユーザ クレデンシャルの検証で、認証サーバからユーザ アトリビュートを受信します。返されたユーザ アトリビュートにクラス アトリビュートが含まれる場合、セキュリティ アプライアンスはアトリビュートをそのユーザのグループ ポリシーとして解釈し、グループ アトリビュートを取得するためにこのグループ ポリシーに設定されている AAA サーバ グループに要求を送信します。

ステップ 7　**Add** をクリックして、アトリビュート マップに名前のマッピングを加えます。

ステップ 8　**Map Value** タブをクリックしてから、Map Value タブ上の **Add** をクリックします。

図 6-4 のように、Add LDAP Attributes Map Value ダイアログボックスが表示されます。

図 6-4　Add LDAP Attributes Map Value ダイアログボックス



ステップ 9　Custom Name メニューから、値をマッピングするカスタム アトリビュートを選択します。

ステップ 10　Custom Value フィールドに、カスタム（ユーザ定義の）値を入力します。

ステップ 11　Cisco Value フィールドにシスコの値を入力します。

ステップ 12　**Add** をクリックして、アトリビュート マップに値のマッピングを追加します。

ステップ 13　マッピングするそれぞれのアトリビュートの名前と値に対して、ステップ 4 からステップ 12 を繰り返します。

ステップ 14　すべての名前と値のマッピングが完了したら、Add LDAP Attribute Map ウィンドウの一番下にある **OK** をクリックします。

ステップ 15　**Apply** をクリックして、新しい LDAP アトリビュート マップを完了し、セキュリティ アプライアンスの実行コンフィギュレーションに追加します。

AAA サーバ グループと AAA サーバの設定

次に、使用する AAA サーバ グループと AAA サーバを設定します。2 つの AAA サーバ グループを設定する必要があります。1 つのサーバ グループは、ユーザ レコードの LDAP 検索を要求する認証サーバを含む認証サーバ グループとして設定します。もう 1 つのサーバ グループは、グループ レコードの LDAP 検索を要求する許可サーバを含む許可サーバ グループとして設定します。2 つのグループで大きく異なる点は、AAA サーバに別のベース DN フィールドが存在し、別の Active Directory フォルダを指定して検索を行うところです。

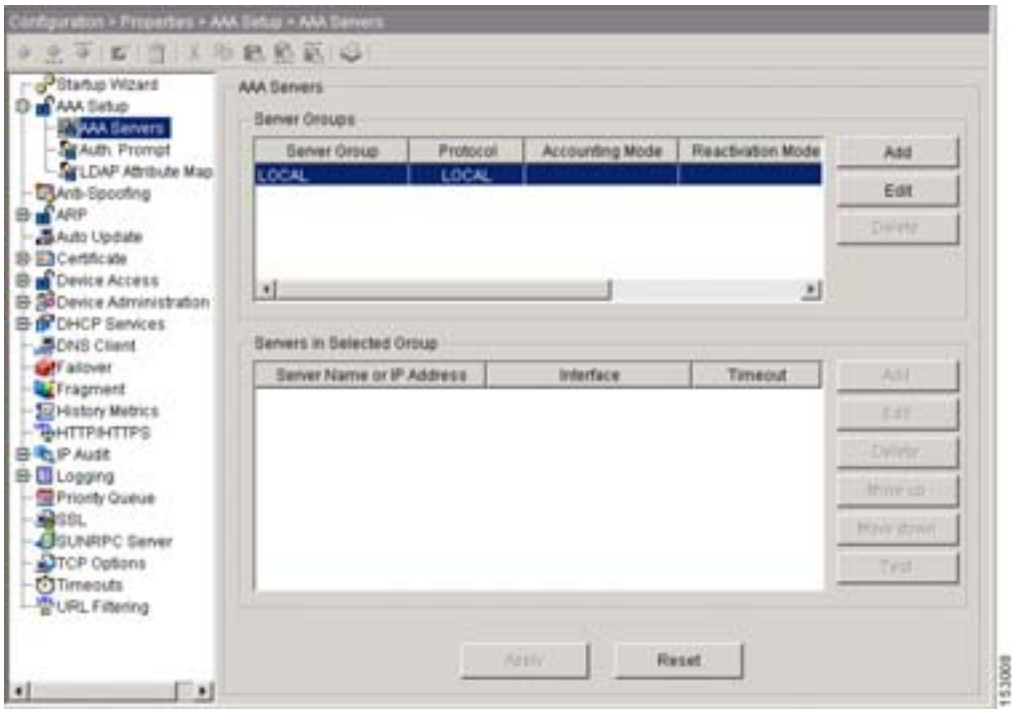
LDAP AAA サーバ グループの作成

2 つのサーバ グループを設定するには、次の手順を実行します。

ステップ 1　Cisco ASDM ウィンドウで、**Configuration > Properties > AAA Setup > AAA Servers** を選択します。

図 6-5 のように、ウィンドウの右側に AAA Servers 領域が表示されます。

図 6-5　AAA Servers を選択した ASDM ウィンドウ

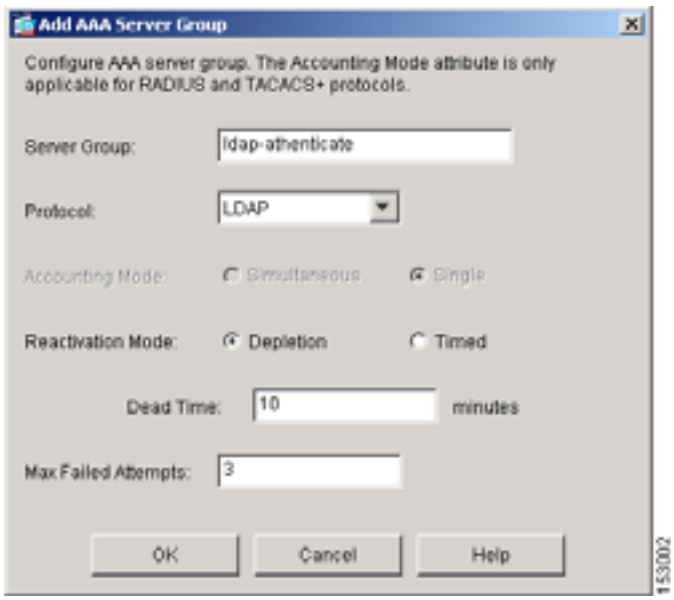


AAA Servers 領域内のフィールドは、Server Groups 領域と Servers In The Selected Group 領域の 2 つの領域に分けられます。Server Groups 領域では、セキュリティ アプライアンスが各グループに表示されたサーバと通信を行うのために使用する AAA サーバ グループとプロトコルを設定できます。

ステップ 2　Server Groups 領域で **Add** をクリックします。

図 6-6 のように、Add AAA Server Group ダイアログボックスが表示されます。

図 6-6　Add AAA Server Group ダイアログボックス



ステップ 3　Server Group フィールドにサーバ グループの名前を入力します。

認証サーバ グループと許可サーバ グループには、別個の名前を使用してください。この例では、認証サーバ グループに *ldap-authenticat*（最大文字数が 16 のため、authenticate の最後の文字を切り詰めています）、許可サーバ グループに *ldap-authorize* という名前が付けられています。

ステップ 4　Protocol メニューから **LDAP** を選択します。

ステップ 5　Reactivation Mode では、次のいずれかを選択します。

- **Depletion**：グループ内のすべてのサーバが非アクティブになった場合にだけ、失敗したサーバを再度アクティブにするようにセキュリティ アプライアンスを設定します。
- **Timed**：30 秒のダウン タイムの後、失敗したサーバを再度アクティブにするようにセキュリティ アプライアンスを設定します。

ステップ 6　Dead Time フィールドに、グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度アクティブにするまでの経過時間を分数で入力します。

このフィールドは、ステップ 5 で Timed モードを選択した場合には使用できません。

ステップ 7　Max Failed Attempts フィールドに、応答が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失敗の回数（1 ～ 5）を入力します。

ステップ 8　**OK** をクリックして、新しく設定したサーバを Server Groups テーブルに入力します。

ステップ 9　もう 1 つの AAA サーバ グループに対して、ステップ 2 からステップ 8 を繰り返します。この作業を完了すると、認証サーバ グループと許可サーバ グループが作成されています。

LDAP AAA サーバの設定

次に、2 つの AAA サーバ グループのそれぞれに対して、AAA サーバを設定します。ここでも、1 つのサーバは認証用で、もう 1 つのサーバは許可用です。

AAA サーバ グループのそれぞれに新しい LDAP AAA サーバを追加するには、次の手順を実行します。

ステップ 1　Cisco ASDM ウィンドウで、**Configuration > Properties > AAA Setup > AAA Servers** を選択します。

ウィンドウの右側に AAA Servers 領域が表示されます。

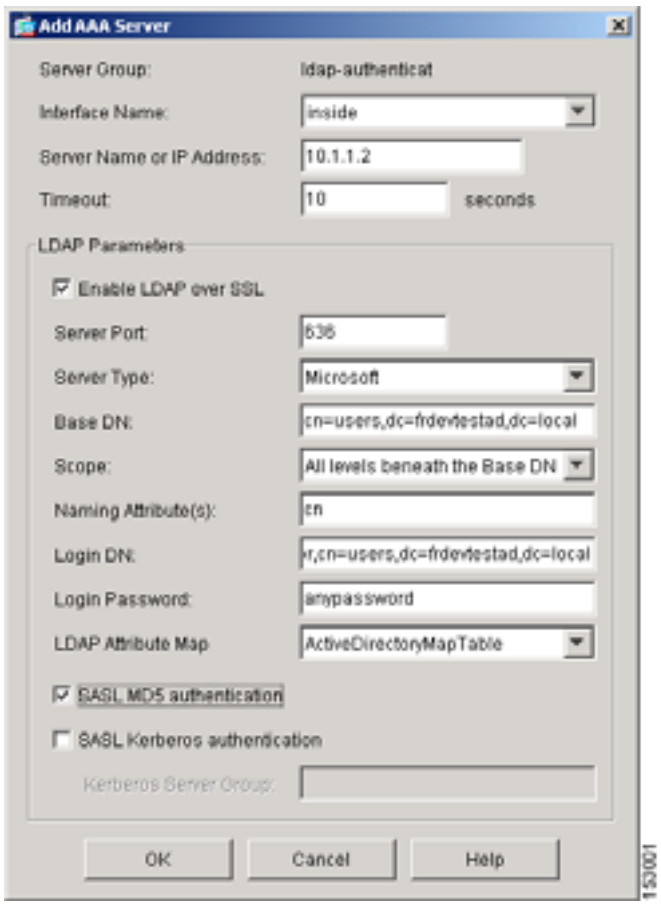
ステップ 2　Server Group テーブルで、LDAP サーバを追加する LDAP サーバ グループをクリックします。

この例では、認証サーバを ldap-authenticat グループに、許可サーバを ldap-authorize グループに設定します。

ステップ 3　Servers in Selected Group 領域で **Add** をクリックします。

図 6-7 のように、Add AAA Server ダイアログボックスが表示されます。

図 6-7　Add AAA Server ダイアログボックス



ステップ 4　Interface Name メニューから、次のいずれかを選択します。

- **Inside**：LDAP サーバが内部ネットワーク上にある場合
  または
- **Outside**：LDAP サーバが外部ネットワーク上にある場合

この例では、LDAP サーバは内部ネットワーク上にあります。

ステップ 5　Server Name or IP Address フィールドに、サーバ名または IP アドレスを入力します。

この例では、IP アドレスを使用します。

ステップ 6　Timeout フィールドに、タイムアウト間隔を秒単位で入力します。

この時間に達すると、セキュリティ アプライアンスはプライマリ AAA サーバに対する要求の送信を放棄します。サーバ グループにスタンバイ サーバがある場合、セキュリティ アプライアンスは要求をバックアップ サーバに送信します。

ステップ 7　セキュリティ アプライアンスと LDAP ディレクトリ間のすべての通信を SSL で暗号化する場合は、LDAP Parameters 領域の **Enable LDAP over SSL** をオンにします。

警告　**Enable LDAP over SSL をオンにしない場合、セキュリティ アプライアンスと LDAP ディレクトリは、機密の認証データと許可データを含むすべてのデータを暗号化せずに交換します。**

ステップ 8　Server Port フィールドに、使用するサーバ ポートを入力します。

これは、サーバにアクセスするための TCP ポート番号です。

ステップ 9　Server Type メニューから、次のいずれかを選択します。

- **Sun Microsystems JAVA System Directory Server**（以前の Sun ONE Directory Server）
  または
- **Microsoft Active Directory**
  または
- **Detect automatically**

セキュリティ アプライアンスは、Sun Microsystems JAVA System Directory Server（以前の名前は Sun ONE Directory Server）と Microsoft Active Directory でのみ、認証とパスワード管理の機能をサポートしています。Detect automatically を選択することにより、サーバが Microsoft であるか Sun サーバであるかの判断をセキュリティ アプライアンスに委ねることができます。

（注）　Sun Directory Server にアクセスするためにセキュリティ アプライアンスに設定されている DN は、そのサーバ上のデフォルトのパスワード ポリシーにアクセスできる必要があります。DN にディレクトリ管理者または、ディレクトリ管理者の権限を持つユーザを使用することを推奨します。または、デフォルトのパスワード ポリシーに ACI を適用できます。

ステップ 10 Base DN フィールドに、次のいずれかを入力します。

- 認証サーバを設定する場合は、ユーザ アトリビュートを保有する Active Directory フォルダのベース DN（通常、ユーザ フォルダ）

  または

- 許可サーバを設定する場合は、グループ アトリビュートを保有する Active Directory フォルダのベース DN（通常、グループ フォルダ）

ベース DN は、許可要求を受信したときに、サーバが検索を開始する LDAP 階層に位置します。たとえば、OU=people, dc=cisco, dc=com となります。

ステップ 11 Scope メニューから、次のいずれかを選択します。

- **One level beneath the Base DN**

  または

- **All levels beneath the Base DN**

このスコープは、許可要求を受信したサーバに検索させる LDAP 階層の範囲を指定します。One Level Beneath the Base DN は、Base DN の 1 つ下のレベルだけを指定します。このオプションは、時間がかかりません。All Levels Beneath the Base DN は、すべてのサブツリー階層の検索を指定します。このオプションは、多少時間がかかります。

ステップ 12 Naming Attribute(s) フィールドに、LDAP サーバ上のエントリを一意に識別する Relative Distinguished Name アトリビュートを入力します。

共通の名前付きアトリビュートは、Common Name（cn）と User ID（uid）です。

ステップ 13 Login DN フィールドで、次のいずれかを実行します。

- セキュリティ アプライアンスの認証バインディングに対するディレクトリ オブジェクトの名前を入力します。たとえば、cn=Administrator, cn=users, ou=people, dc=Example Corporation, dc=com と入力します。

  または

- 匿名アクセスの場合は、このフィールドをブランクのままにしておきます。

Microsoft Active Directory サーバなど、一部の LDAP サーバは、セキュリティ アプライアンスが認証バインディングを通じてハンドシェイクの確立を要求してから、LDAP オペレーションの要求を受け入れます。セキュリティ アプライアンスは、認証バインディングに対して、Login DN フィールドをユーザ認証要求に付加して、自身を識別します。Login DN フィールドは、セキュリティ アプライアンスの認証特性を定義します。これらの特性は、管理者の権限が与えられているユーザの特性に対応します。

ステップ 14 Login Password フィールドに、Login DN に関連付けられているパスワードを入力します。

入力する文字は、アスタリスクで表示されます。

ステップ 15 LDAP Attribute Map メニューから、LDAP サーバに適用する LDAP アトリビュート マップを選択します。

LDAP アトリビュート マップは、ユーザ定義の LDAP アトリビュート名および値と、シスコのアトリビュート名および値を変換します。新しい LDAP アトリビュート マップを設定するには、P.6-3 の「LDAP アトリビュート マップの作成」を参照してください。

ステップ 16　**SASL MD5 Authentication** をオンにし、Simple Authentication and Security Layer（SASL）の MD5 メカニズムを使用して、セキュリティ アプライアンスと LDAP サーバ間の認証通信を保護します。

ステップ 17　**SASL Kerberos Authentication** をオンにし、SASL の Kerberos メカニズムを使用して、セキュリティ アプライアンスと LDAP サーバ間の認証通信を保護します。

（注）　サーバに複数の SASL 方式を設定する場合、セキュリティ アプライアンスは、サーバとセキュリティ アプライアンスの両方でサポートされている最も強固な方式を使用します。たとえば、サーバとセキュリティ アプライアンスで MD5 と Kerberos の両方がサポートされている場合、セキュリティ アプライアンスは、サーバとの通信を保護するのに Kerberos を選択します。

ステップ 18　ステップ 17 で SASL Kerberos authentication をオンにした場合は、Kerberos Server Group フィールドに、認証用の Kerberos サーバ グループを入力します。

ステップ 19　ステップ 3 からステップ 18 を繰り返し、もう 1 つの AAA サーバ グループに AAA サーバを設定します。

LDAP 許可に対するグループ ポリシーの設定

LDAP アトリビュート マップ、AAA サーバ グループ、およびグループ内の LDAP サーバを設定したら、次にグループ名と LDAP 許可サーバとを関連付ける外部グループ ポリシーを作成します。

(注)　グループ　ポリシーを設定する総合的な手順は、このマニュアルの他の部分で提供します。次の手順は、LDAP による AAA を設定する場合にだけ適用されます。

新しいグループ ポリシーを作成し、そのグループ ポリシーに LDAP 許可サーバ グループを割り当てるには、次の手順を実行します。

ステップ 1　Cisco ASDM ウィンドウで、**Configuration > VPN > General > Group Policy** を選択します。

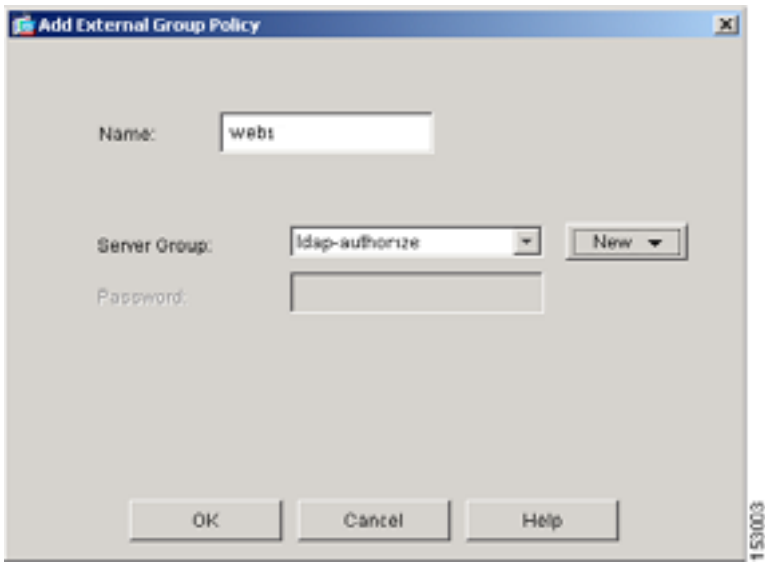
ウィンドウの右側に Group Policy 領域が表示されます。

ステップ 2　**Add** をクリックし、**Internal Group Policy** または **External Group Policy** をクリックします。

この例では、LDAP サーバがセキュリティ アプライアンスの外部にあるため、External Group Policy を選択します。

図 6-8 のように、Add Group Policy ダイアログボックスが表示されます。

図 6-8　Add Group Policy ダイアログボックス



ステップ 3　Name フィールドに新しいグループ ポリシーの名前を入力します。

この例では、グループ ポリシーの名前は *web1* です。

ステップ 4　Server Group メニューから、作成した AAA 許可サーバ グループを選択します。

この例では、ldap-authorize の名前が付いたサーバ グループとなります。

ステップ 5　**OK** をクリックしてから、**Apply** をクリックして、新しいグループ ポリシーを作成します。

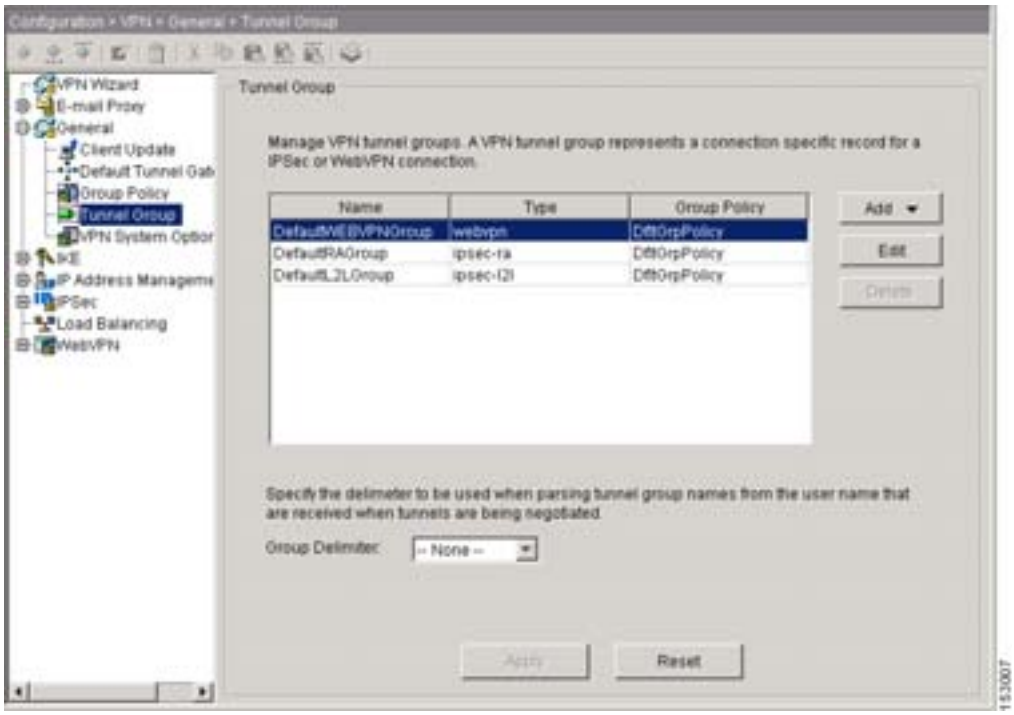
LDAP 認証に対するトンネル グループの設定

最後の主要なタスクでは、次の手順を実行して、LDAP 認証を指定するトンネル グループを作成します。

ステップ 1　Cisco ASDM ウィンドウで、**Configuration > VPN > General > Tunnel Group** を選択します。

図 6-9 のように、ASDM ウィンドウの右側に Tunnel Group 領域が表示されます。

図 6-9　Tunnel Group 領域



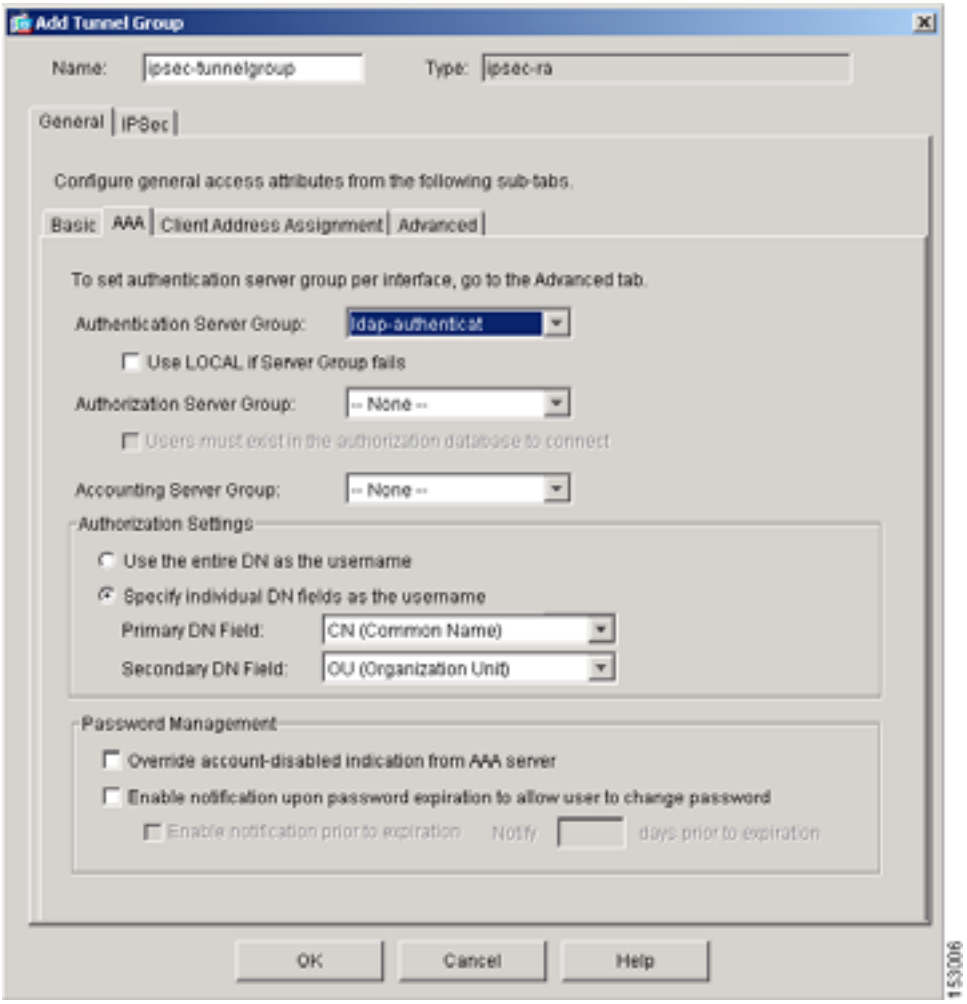
ステップ 2　Tunnel Group 領域で **Add** をクリックし、トンネル グループのタイプを選択します。

この例では、リモート アクセス用の IPSec を選択します。

Add Tunnel Group ダイアログボックスが表示されます。

ステップ 3　図 6-10 のように、**General** タブを選択してから、**AAA** タブを選択します。

図 6-10　General タブと AAA タブを選択した Add Tunnel Group ダイアログボックス



ステップ 4　Name フィールドにトンネル グループの名前を入力します。

この例では、トンネル グループ名は ipsec-tunnelgroup です。

ステップ 5　Authentication Server Group メニューから、認証用に設定した AAA サーバ グループを選択します。

この例では、認証サーバ グループの名前は ldap-authenticat です。

ステップ 6　Add Tunnel Group ダイアログボックスの一番下にある **OK** をクリックします。

ステップ 7　ASDM ウィンドウの一番下にある **Apply** をクリックして、実行コンフィギュレーションに変更内容を加えます。

LDAP 認証と許可用にセキュリティ アプライアンスを設定するために必要な最低限の手順が完了しました。

Citrix MetaFrame サービスの設定

WebVPN ユーザは、セキュリティ アプライアンスとの接続を通じて、Citrix MetaFrame サービスにアクセスできます。次の項では、この機能の紹介、前提条件の提示、この機能をサポートするようにセキュリティ アプライアンスを設定するための ASDM の使用方法についての説明を行っています。

(注) この章の手順の実行中に、ASDM ウィンドウに表示されるアトリビュートの詳細を参照するには、**Help** をクリックしてください。

概要

セキュリティ アプライアンスを使用すると、Citrix Independent Computing Architecture（ICA）クライアントは、WebVPN 接続で Citrix Presentation Server を実行している企業エンタープライズ アプリケーションにアクセスできます。WebVPN ホーム ページを Citrix Web サーバにリダイレクトしたり、サーバへのリンクを WebVPN ホーム ページに追加したり、サーバの URL を入力して Citrix MetaFrame サービスにアクセスするようにユーザに指示したりできます。WebVPN ユーザが Citrix Web サーバに接続されると、Citrix Web Interface はユーザを認証し、ユーザによる企業リソースへのアクセスが可能になります。

（注） この設定では、セキュリティ アプライアンスは Citrix セキュア ゲートウェイとして機能します。

1 つ以上の Citrix Presentation Server で実行される Citrix MetaFrame サービスに対するセキュリティ アプライアンス サポートを設定するには、次の項の手順を実行します。

始める前に

この章の手順を実行する前に、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します。

（注） Citrix サーバに接続するすべてのブラウザは、128 ビット暗号化をサポートしている必要があります。

トラストポイントの追加

この項の手順では、セキュリティ アプライアンスの設定にトラストポイントを追加して、Citrix 接続要件を満たす方法を説明します。

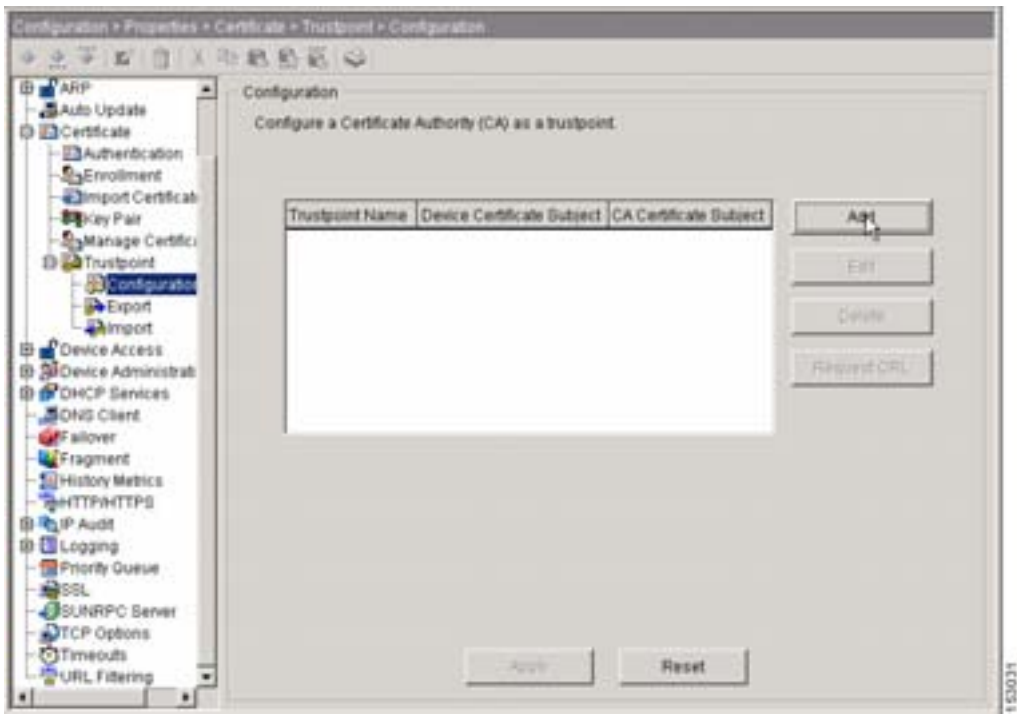
トラストポイントは、certificate authority（CA; 認証局）の ID、CA 固有の設定パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションを含んでいます。Citrix サーバに接続するにはトラストポイントが 1 つ必要です。セキュリティ アプライアンス上の異なるインターフェイスにそれぞれを割り当てて、最大 2 つのトラストポイントを設定できますが、2 つのインターフェイスに 1 つのトラストポイントを割り当てることもできます。

セキュリティ アプライアンス設定にトラストポイントを追加する手順は、次のとおりです。

ステップ 1　Configuration > Properties > Certificate > Trustpoint > Configuration を選択します。

Trustpoint Configuration ウィンドウが開きます（図 7-1）。

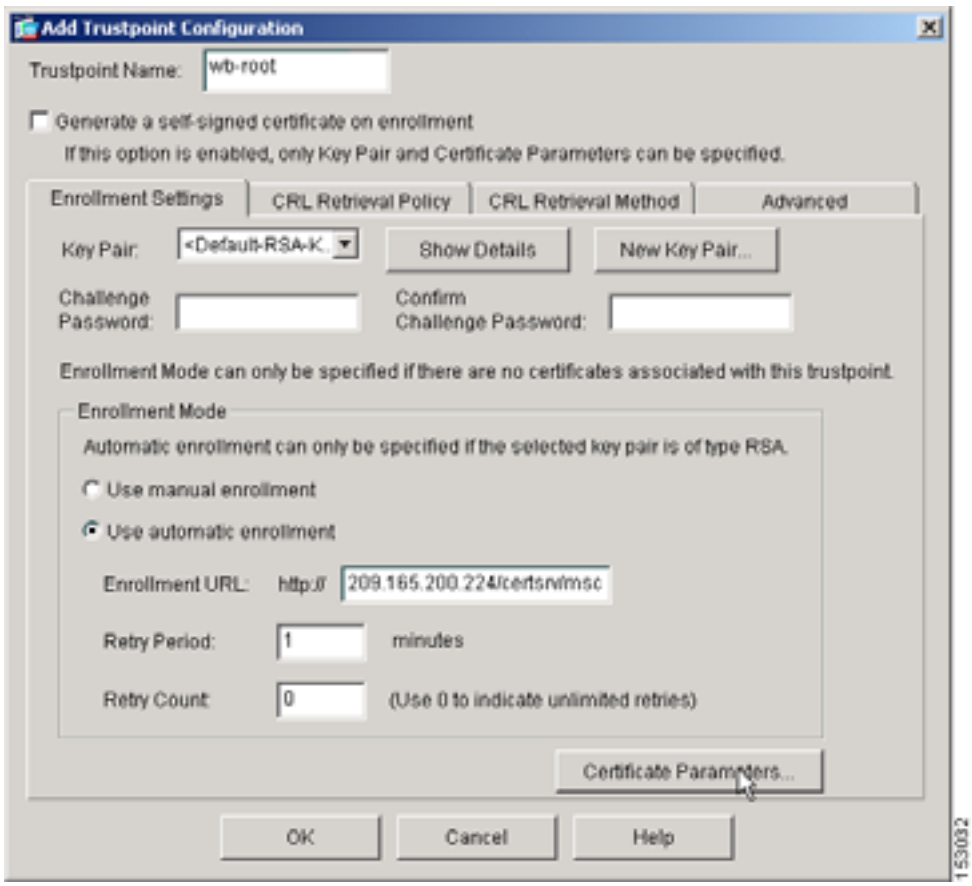
図 7-1　Trustpoint Configuration



ステップ 2　**Add** をクリックします。

Add Trustpoint Configuration ウィンドウが開きます（図 7-2）。

図 7-2　Add Trustpoint Configuration



ステップ 3　**Trustpoint Name** フィールドに証明書の名前などの値を入力して、このトラストポイントを一意に識別し、証明書に視覚的にわかりやすいアソシエーションを提供します。

ステップ 4　次のいずれかのアトリビュートをオンにします。

- **Use manual enrollment**

  このオプションは、PKCS10 証明書要求を生成することを指定します。CA は要求に基づいてセキュリティ アプライアンスに証明書を発行し、新しい証明書をインポートすることによって、セキュリティ アプライアンスに証明書がインストールされます。

- **Use automatic enrollment**

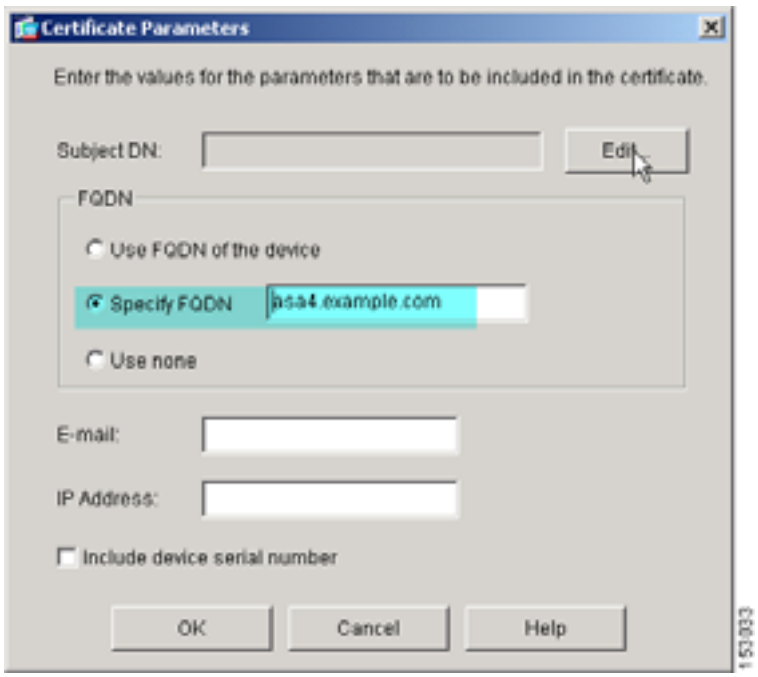
  このオプションを選択する場合、**Enrollment URL** フィールドに自動登録用の URL を入力します。

  自動登録オプションは、SCEP モードを使用することを指定します。トラストポイントが SCEP 登録用に設定されている場合、セキュリティ アプライアンスは SCEP プロトコルを使用して証明書をダウンロードします。

ステップ 5　**Certificate Parameters** をクリックします。

Certificate Parameters ウィンドウが開きます（図 7-3）。

図 7-3　Certificate Parameters



ステップ 6　**Specify FQDN** をオンにします。

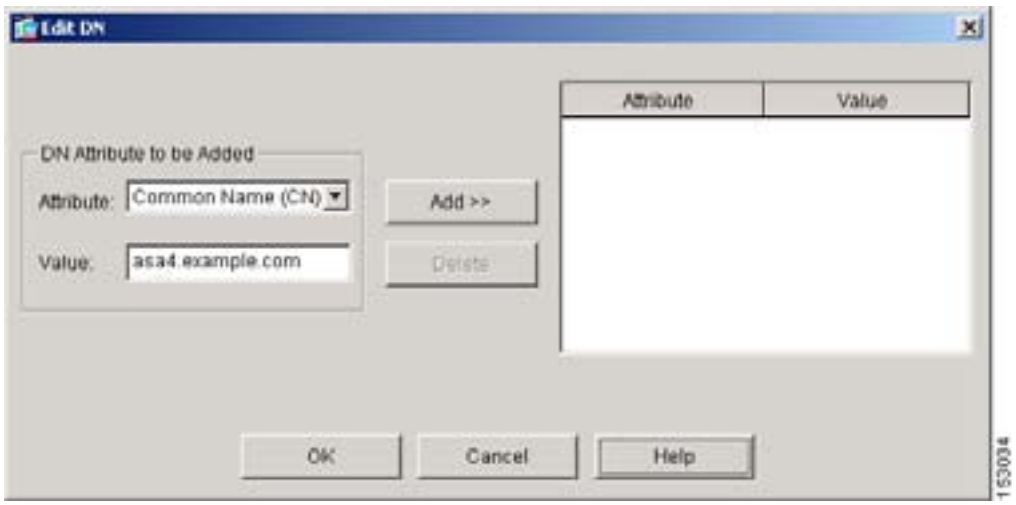
ステップ 7　**Specify FQDN** フィールドに、証明書の Subject Alternative Name 拡張子で使用する Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を入力します。

FQDN は、要求を送信するアドレスをサーバ プログラムに指定します。

ステップ 8　**Edit** をクリックします。

Edit DN ウィンドウが開きます（図 7-4）。

図 7-4　Edit DN



ステップ 9　**Attribute** フィールドの隣にあるドロップダウン リストから **Common Name（CN）**を選択します。

ステップ 10　**Value** フィールドにステップ 6 で入力した FQDN を入力して、**Add** をクリックします。

Citrix ICA 接続アプリケーションでは、SSL 証明書の Common Name（CN）フィールドで FQDN が必要となります。

注意　CN として IP アドレスを指定しないでください。

ASDM は、右側のテーブルに新しいエントリを挿入します。

ステップ 11　**OK** を 3 回クリックします。

ASDM は、Trustpoint Configuration テーブルに新しいトラストポイントを挿入します（図 7-1）。

ステップ 12　**Apply** をクリックして、トラストポイントをフラッシュ デバイスに保存します。

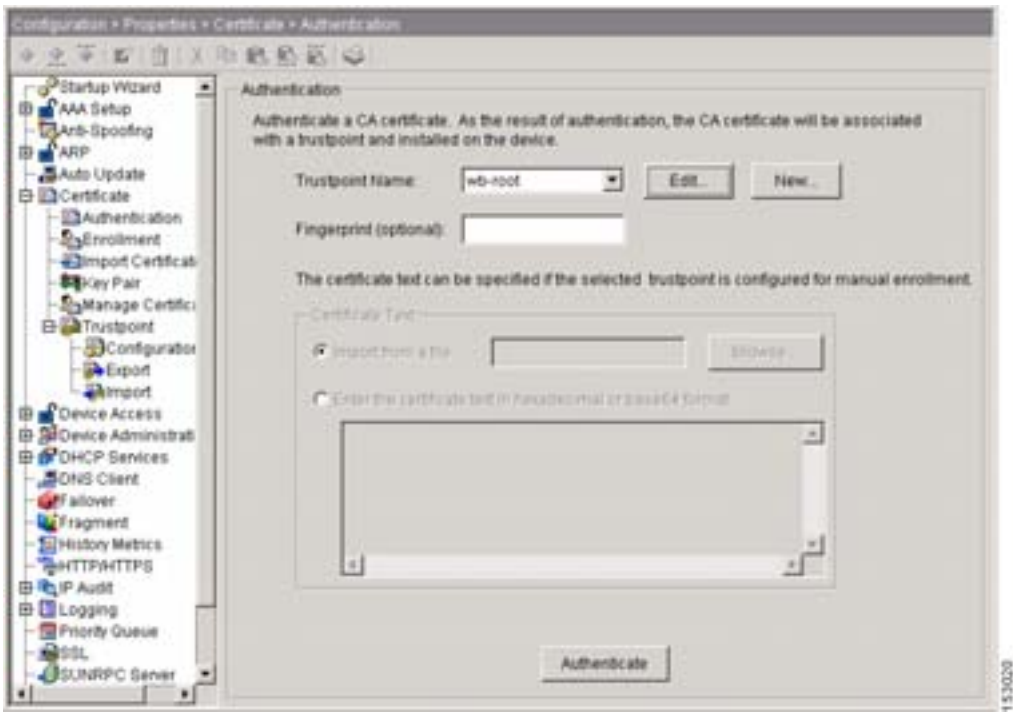
認証局の認証

これでトラストポイントが追加されたため、次は認証局を認証する必要があります。手順は次のとおりです。

ステップ 1　Configuration > Properties > Certificate > Authentication を選択します。

Authentication ウィンドウが開きます（図 7-5）。

図 7-5　Authentication



ステップ 2　**Trustpoint Name** アトリビュートの隣にあるドロップダウン リストから前の項で作成したトラストポイントを選択します。

ステップ 3　**Authenticate** をクリックします。

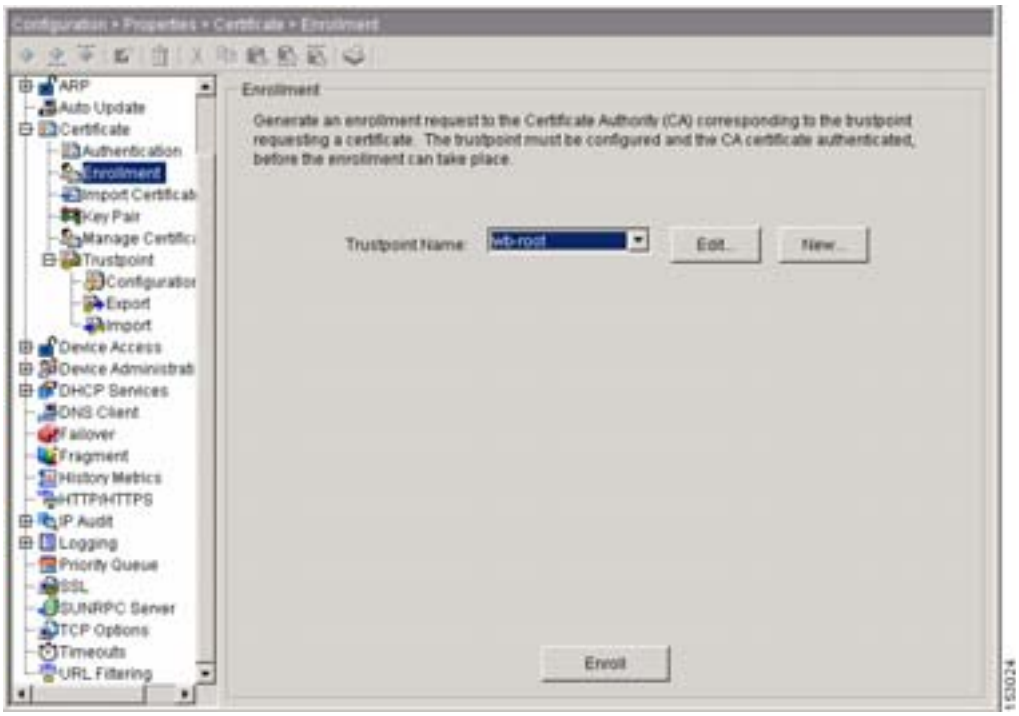
証明書の登録

証明書を登録する場合、トラストポイントに関連付けられるように証明書を指定します。証明書を登録し、Citrix 接続で使用されるようにします。手順は次のとおりです。

ステップ 1　Configuration > Properties > Certificate > Enrollment を選択します。

Enrollment ウィンドウが開きます（図 7-6）。

図 7-6　Enrollment



ステップ 2　**Trustpoint Name** アトリビュートの隣にあるドロップダウン リストから前の項で作成したトラストポイントを選択します。

ステップ 3　**Enroll** をクリックします。

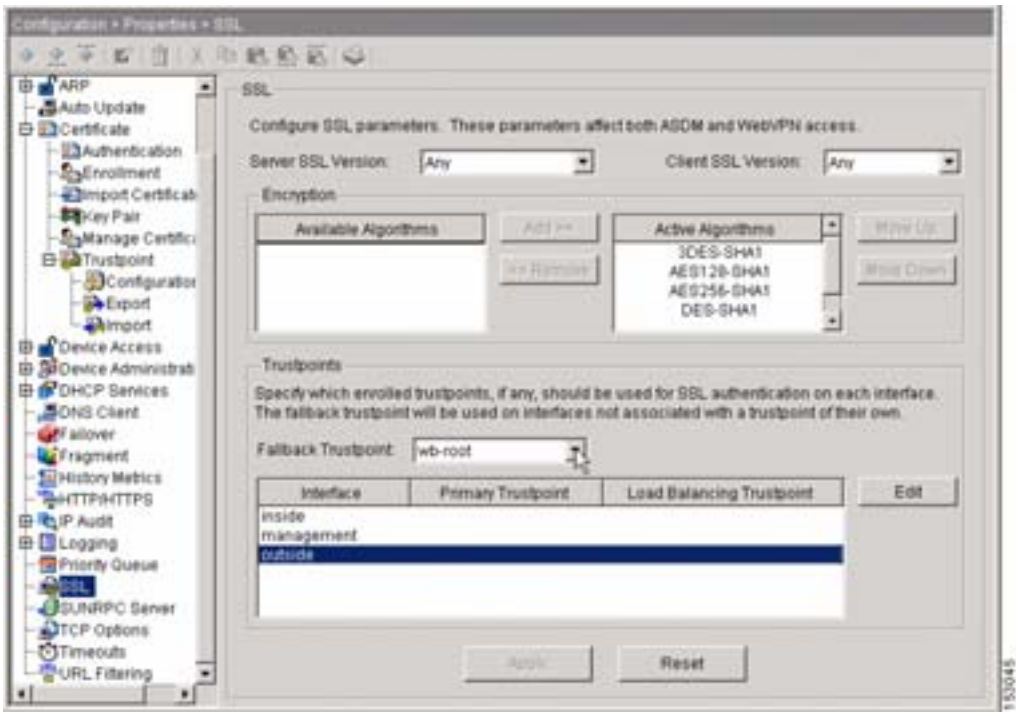
インターフェイスへのトラストポイントの適用

この項の手順では、Citrix サーバに対する WebVPN セッションを終了するために使用するセキュリティ アプライアンス インターフェイスにトラストポイントを適用する方法を説明します。このインターフェイスを Citrix 接続専用にすることはできますが、必ずしも必要ではありません。インターフェイスをトラストポイントに適用する手順は、次のとおりです。

ステップ 1　Configuration > Properties > SSL を選択します。

SSL ウィンドウが開きます（図 7-7）。

図 7-7　SSL



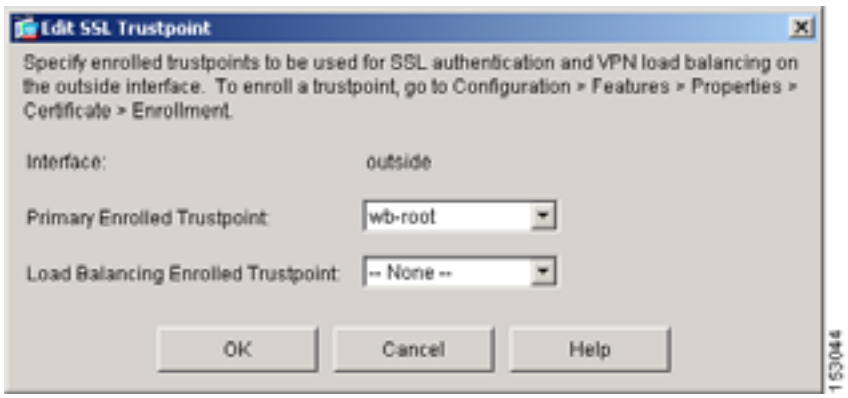
ステップ 2　次のいずれかの内容を実行します。

- インターフェイスに特定のトラストポイントが割り当てられていない場合に、トラストポイントを使用するようにインターフェイスを設定するには、**Fallback Trustpoint** アトリビュートの隣にあるトラストポイントを選択してから、**Apply** をクリックし、設定変更をフラッシュ デバイスに保存します。このステップで、インターフェイスへのトラストポイントの割り当てが完了します。
- Citrix サーバに対する WebVPN セッションを終了するために使用するインターフェイスをダブルクリックし、インターフェイスにトラストポイントを明示的に割り当てます。

  通常、これらのセッションを終了するために使用されるインターフェイスは外部インターフェイスです。

  Edit SSL Trustpoint ウィンドウが開きます（図 7-8）。

図 7-8　Edit SSL Trustpoint



ステップ 3　**Primary Enrolled Trustpoint** アトリビュートの隣にあるトラストポイントを選択して、**OK** をクリックしてから、**Apply** をクリックし、設定変更をフラッシュ デバイスに保存します。

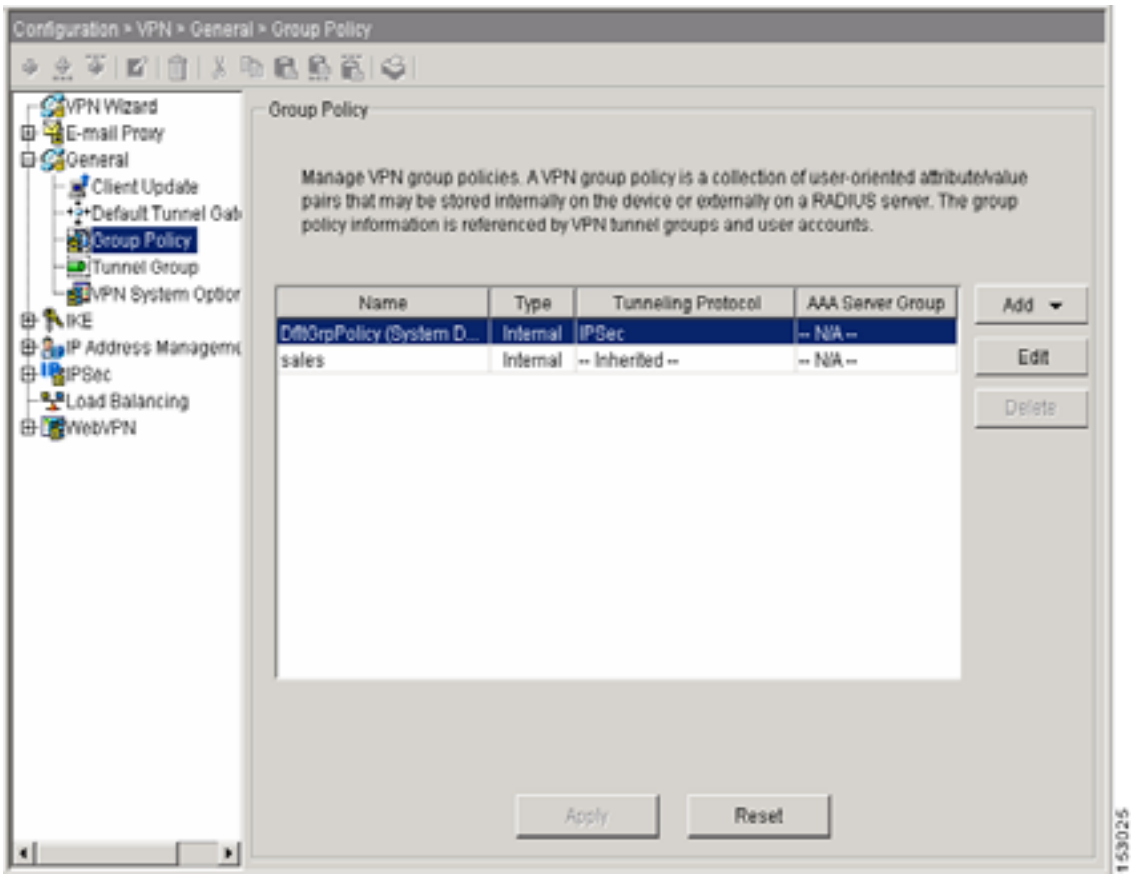
WebVPN のイネーブル化

Citrix MetaFrame サービスにリモート アクセスするには、WebVPN トンネリングをイネーブルにする必要があります。これらのサービスを提供するユーザに適用されているグループ ポリシー上の WebVPN をイネーブルにする手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Group Policy を選択します。

Group Policy ウィンドウが開きます（図 7-9）。

図 7-9　Group Policy



ステップ 2　次のいずれかの方法を使用します。

- デフォルトのグループ ポリシーを設定して、WebVPN トンネリングをイネーブルにする。

  デフォルトでは、グループ ポリシーとユーザはデフォルトのグループ ポリシーの設定を継承します。

  Group Policy テーブル内の DfltGrpPolicy エントリをダブルクリックし、General タブが開いていることを確認してから、Tunneling Protocols の隣にある **WebVPN** をオンにして、**OK** をクリックします。

- Citrix MetaFrame サービスを提供する代替グループ ポリシーに WebVPN を制限する。

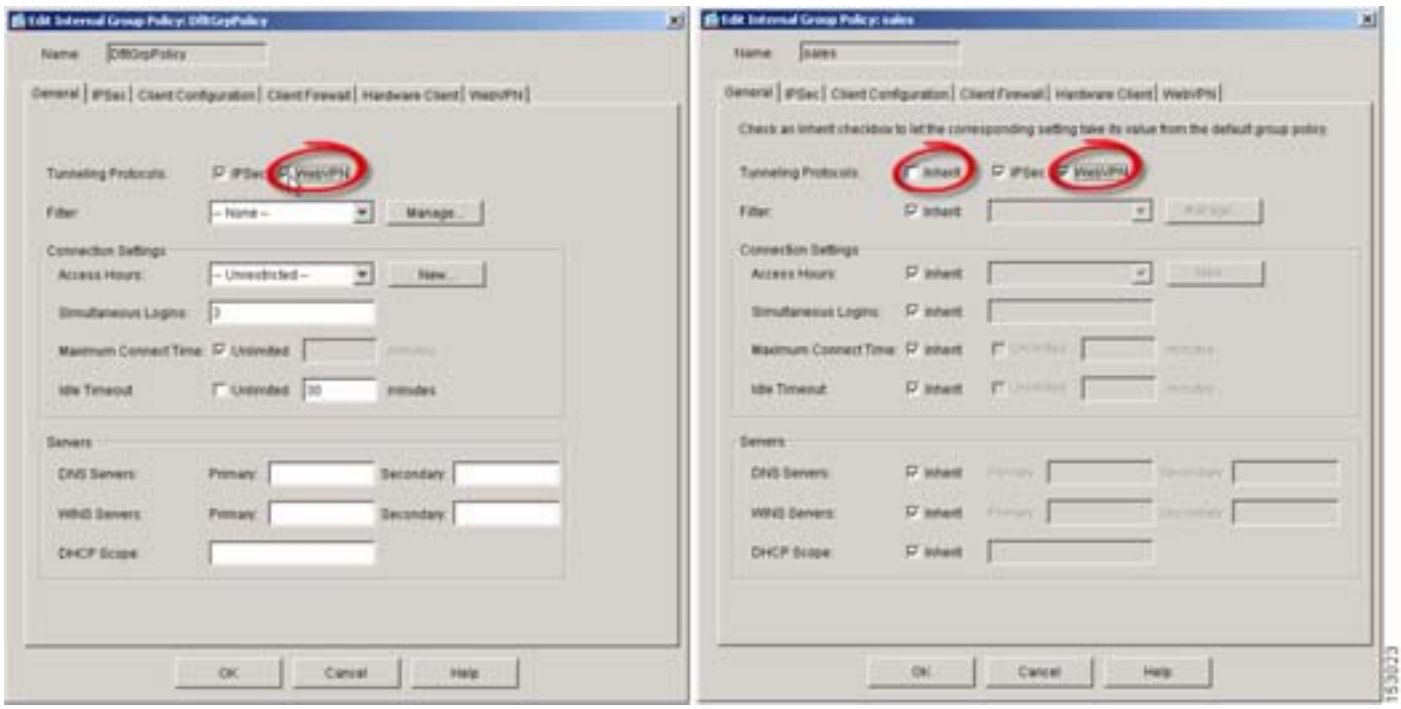
  デフォルトでは、ユーザは割り当てられたグループ ポリシーからトンネリング プロトコルを継承します。

  Citrix MetaFrame サービスへのアクセスを提供する各内部または外部のグループ ポリシーで、Group Policy テーブル内のポリシーをダブルクリックし、General タブが開いていることを確認してから、Tunneling Protocols の隣にある **Inherit** チェックボックスをオフにし、**WebVPN** をオンにして、**OK** をクリックします。

(注) 新しいグループ ポリシーを作成して WebVPN サービスをイネーブルにすることもできますが、その場合は、さらにこのアクセス権を与えるユーザにグループ ポリシーを割り当てる必要があります。グループ ポリシーの設定方法に関する詳細については、第 2 章「グループ ポリシーの設定」を参照してください。

図 7-10 は、DfltGrpPolicy と代替ポリシーの General タブを比較しています。

図 7-10　DfltGrpPolicy と代替グループ ポリシーの WebVPN オプション



(注) 代替グループ ポリシーの Inherit チェックボックスをオンにすると、ポリシーはデフォルト グループ ポリシーの WebVPN 設定を使用します。Inherit チェックボックスをオフにすると、代替グループ ポリシーの WebVPN 設定をカスタマイズでき、デフォルト グループ ポリシーの WebVPN 設定に依存しなくなります。

ステップ 3　**Apply** をクリックして、変更したグループ ポリシーをフラッシュ デバイスに保存します。

Citrix のイネーブル化

デフォルトのグループ ポリシー、代替グループ ポリシー、または個々のユーザ アカウントで Citrix MetaFrame サービスをイネーブルにできます。使用する方法が記載されている項を参照してください。

- グループ ポリシーでの Citrix のイネーブル化（P.7-13）
- ユーザ アカウントでの Citrix のイネーブル化（P.7-15）

グループ ポリシーでの Citrix のイネーブル化

1 つ以上のグループ ポリシーで Citrix MetaFrame サービスをイネーブルにする手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Group Policy を選択します。

Group Policy ウィンドウが開きます。

ステップ 2　次のいずれかの方法を使用して、Citrix MetaFrame サービスをイネーブルにします。

- デフォルトのグループ ポリシーを設定して、Citrix をイネーブルにする。

  デフォルトでは、代替グループ ポリシーとユーザはデフォルトのグループ ポリシーの設定を継承します。

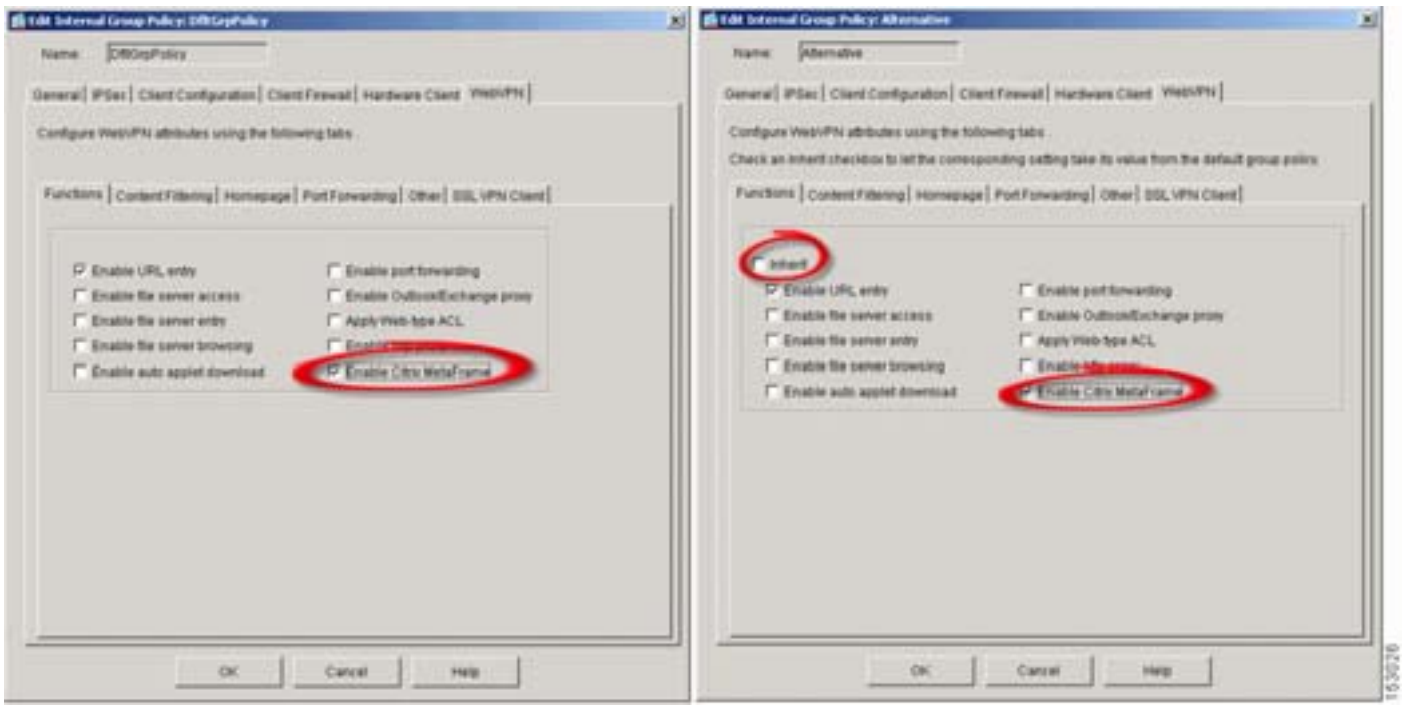
  Group Policy テーブル内の DfltGrpPolicy エントリをダブルクリックして、**WebVPN** > **Functions** タブを開き、**Enable Citrix MetaFrame** をオンにして、**OK** をクリックします。
- Citrix に対するサポートを設定する代替グループ ポリシーを設定して、WebVPN トンネリングをイネーブルにする。

  デフォルトでは、ユーザは割り当てられたそれぞれのグループ ポリシーから Functions 設定を継承します。

  Citrix アクセスをイネーブルにする各内部または外部のグループ ポリシーで、Group Policy テーブル内のポリシーをダブルクリックして、**WebVPN** > **Functions** タブを開き、**Inherit** をオフにしてから、**Enable Citrix MetaFrame** をオンにして、**OK** をクリックします。

図 7-11 は、DfltGrpPolicy と代替ポリシーの WebVPN > Functions タブを比較しています。

図 7-11　DfltGrpPolicy と代替グループ ポリシーでの Citrix MetaFrame のイネーブル化



代替グループ ポリシーの Inherit チェックボックスをオンにすると、ポリシーはデフォルト グループ ポリシーの Enable Citrix MetaFrame を使用します。Inherit チェックボックスをオフにすると、代替グループ ポリシーの Functions 設定をカスタマイズでき、デフォルト グループ ポリシーの WebVPN 設定に依存しなくなります。

ヒント

図 7-11 に示すように Enable URL entry アトリビュートをオンにした場合、リモート ユーザは、WebVPN ホーム ページまたはフローティング ツールバーに Citrix サーバの URL を入力できます。Citrix サーバにホーム ページをリダイレクトしたり、ホーム ページとフローティング ツールバーにリンクを作成したりして、ユーザによる Citrix サーバへの接続を可能にすることもできます。デフォルトでは、Enable URL entry アトリビュートがデフォルトのグループ ポリシーでオンになっています。代替グループ ポリシーで Inherit をオフにすると、ASDM は自動的にチェック マークを挿入してこのアトリビュートをイネーブルにします。ユーザが Citrix サーバの URL を含む URL を入力できるようにするには、デフォルト設定（オン）を使用します。それ以外の場合は、このアトリビュートをオフにします。Citrix サーバへの WebVPN アクセスを提供することが可能なオプションについては、P.7-17 の「Citrix アクセス方法の設定」の項で詳しく説明します。

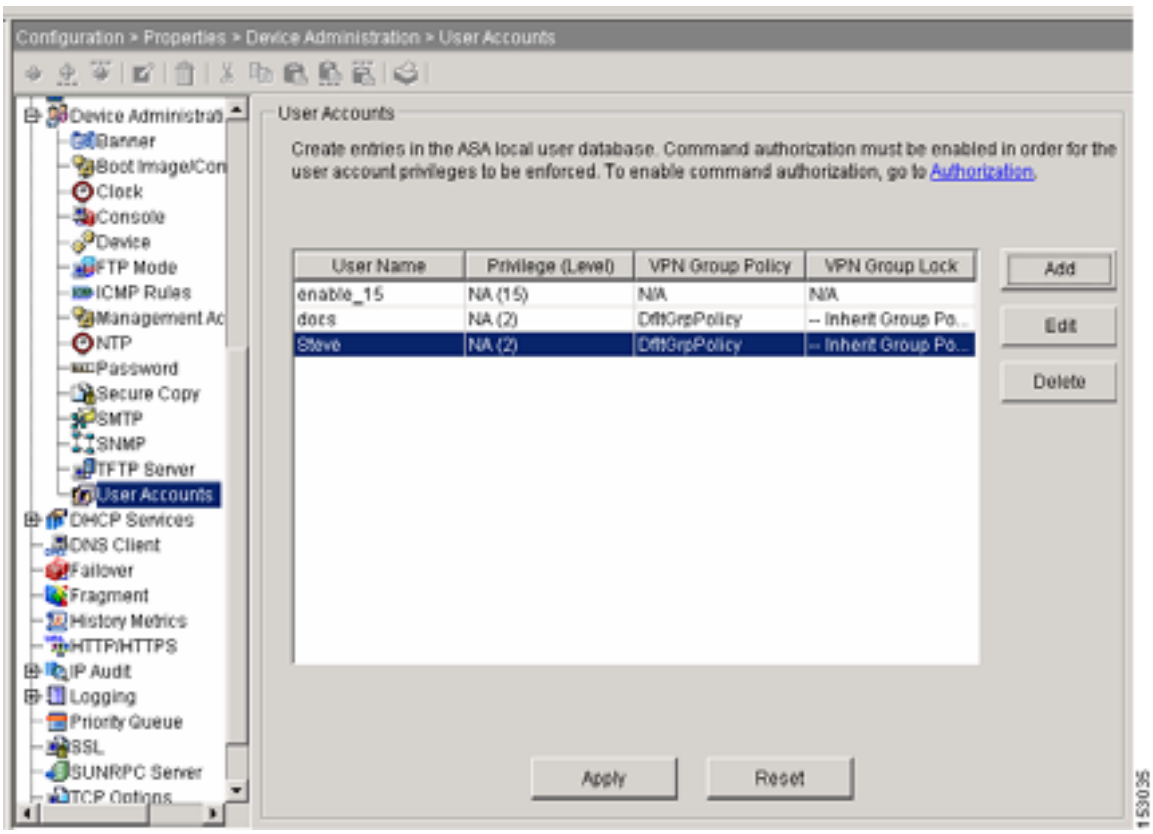
ユーザ アカウントでの Citrix のイネーブル化

ユーザに適用されるグループ ポリシーで Citrix サービスをイネーブルにする代わりに、Citrix MetaFrame サービスをサポートするようにユーザ アカウントを変更できます。変更する各ユーザ アカウントでこの手順を 1 回ずつ実行します。

ステップ 1　Configuration > Properties > Device Administration > User Accounts を選択します。

User Accounts ウィンドウが開きます（図 7-12）。

図 7-12　User Accounts

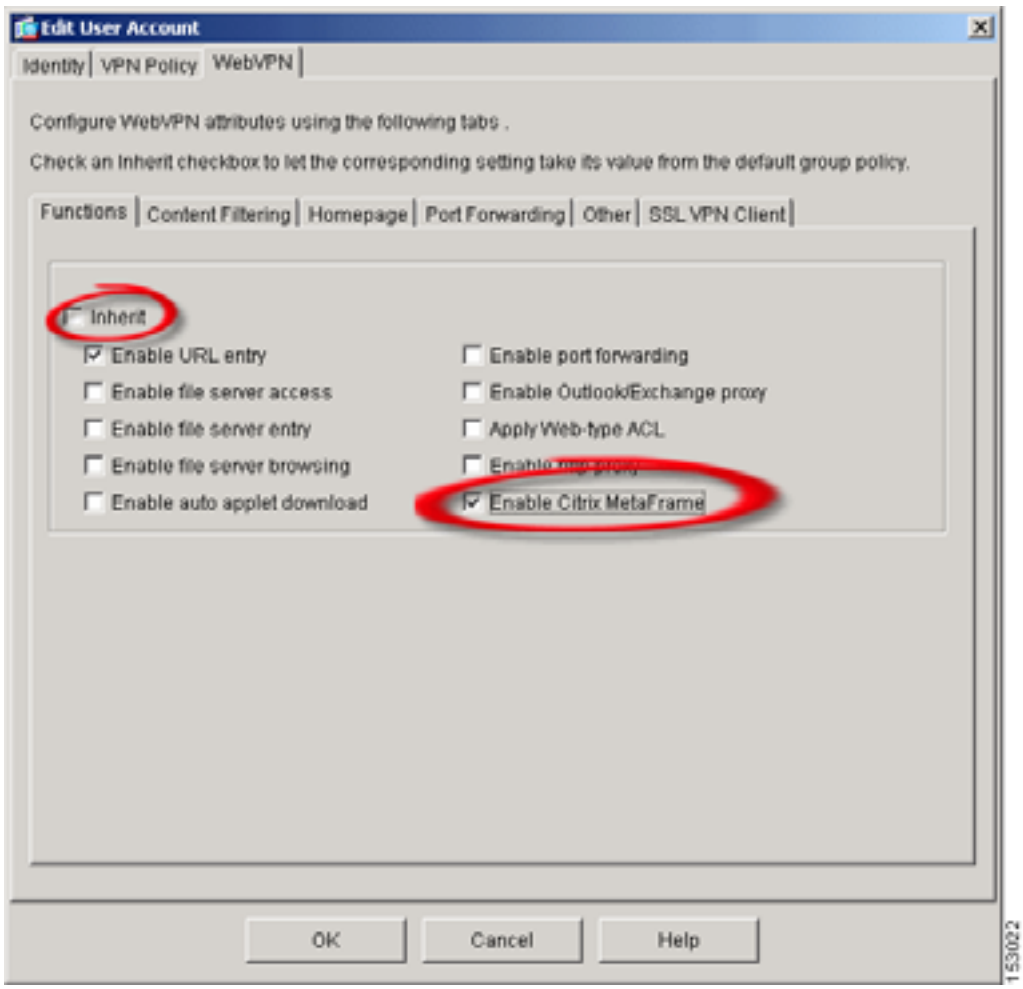


ステップ 2　ユーザ名をダブルクリックします。

ステップ 3　WebVPN > Functions タブを開きます。

WebVPN Functions ウィンドウが開きます（図 7-13）。

図 7-13　Edit User Account：WebVPN の Functions



ステップ 4　**Inherit** チェックボックスをオフにし、**Enable Citrix MetaFrame** をオンにします。

Inherit チェックボックスをオンにすると、ユーザ アカウントは、割り当てられたグループ ポリシーからすべての Functions 設定を使用します。Inherit チェックボックスをオフにすると、そのユーザの Functions 設定をカスタマイズできます。

ステップ 5　他の Functions 設定がそのユーザに適していることを確認します。

ヒント　図 7-13 に示すように Enable URL entry アトリビュートをオンにした場合、ユーザは、WebVPN ホーム ページまたはフローティング ツールバーに Citrix サーバの URL を入力できます。Citrix サーバにホーム ページをリダイレクトしたり、ホーム ページとフローティング ツールバーにリンクを作成したりして、ユーザによる Citrix サーバへの接続を可能にすることもできます。デフォルトでは、Enable URL entry アトリビュートがデフォルトのグループ ポリシーでオンになっています。ユーザ アカウントで Inherit チェックボックスをオフにすると、ASDM は自動的にチェック マークを挿入してこのアトリビュートをイネーブルにします。ユーザが Citrix サーバの URL を含む URL を入力できるようにするには、デフォルト設定（オン）を使用します。それ以外の場合は、このアトリビュートをオフにします。P.7-17 の「Citrix アクセス方法の設定」の項で、Citrix サーバへの WebVPN アクセスを提供することが可能なオプションについて詳しく説明します。

ステップ 6　**OK** をクリックします。

ステップ 7　**Apply** をクリックして、変更したユーザ アカウントをフラッシュ デバイスに保存します。

(注)　Functions 設定の Inherit チェックボックスをオフにしたため、イネーブルになっていた機能にユーザがアクセスできなくなる可能性があります。継承されていた Functions 設定を表示するには、**VPN Policy** タブを開き、Group Policy 設定を書き留めます。Configuration > VPN > General > Group Policy を選択し、表示されていた Group Policy 設定に一致するグループ ポリシー名をダブルクリックしてから、グループ ポリシーの **WebVPN** > **Functions** タブの設定を表示します。

Citrix アクセス方法の設定

ユーザが Citrix MetaFrame サーバに接続できるようにするには、WebVPN ホーム ページまたはツールバー上で実行できるファシリティが必要になります。Citrix サーバに接続するための手段を提供するには、使用する方法が記載されている項を参照してください。

- Citrix サーバへの WebVPN ユーザ ホーム ページのリダイレクト（P.7-17）
- Citrix サーバへのリンクを WebVPN ホーム ページに追加する（P.7-20）
- WebVPN ホーム ページでの URL エントリのイネーブル化（P.7-27）

Citrix サーバへの WebVPN ユーザ ホーム ページのリダイレクト

WebVPN ユーザが Citrix サーバにアクセスできるようにするために、リモート ユーザの WebVPN ホーム ページとして URL を指定することができます。次の項のどれか 1 つを使用して、ホーム ページの URL を変更します。

- グループ ポリシーへのホーム ページのリダイレクト（P.7-17）
- ユーザ アカウントへのホーム ページのリダイレクト（P.7-19）

グループ ポリシーへのホーム ページのリダイレクト

1 つ以上のグループ ポリシーの Citrix MetaFrame サーバの URL に WebVPN ホーム ページをリダイレクトする手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Group Policy を選択します。

Group Policy ウィンドウが開きます。

ステップ 2　次のいずれかの方法を使用して、WebVPN ホーム ページをリダイレクトします。

- デフォルトのグループ ポリシーを設定して、WebVPN ホーム ページをリダイレクトする。

  デフォルトでは、代替グループ ポリシーとユーザはデフォルトのグループ ポリシーの Custom Homepage 設定を継承します。

  Group Policy テーブル内の DfltGrpPolicy エントリをダブルクリックして、**WebVPN** > **Homepage** タブを開き、**Specify URL** をオンにして、ドロップダウン メニューから **http** を選択し、右側のフィールドに Citrix サーバの URL を入力して、**OK** をクリックします。

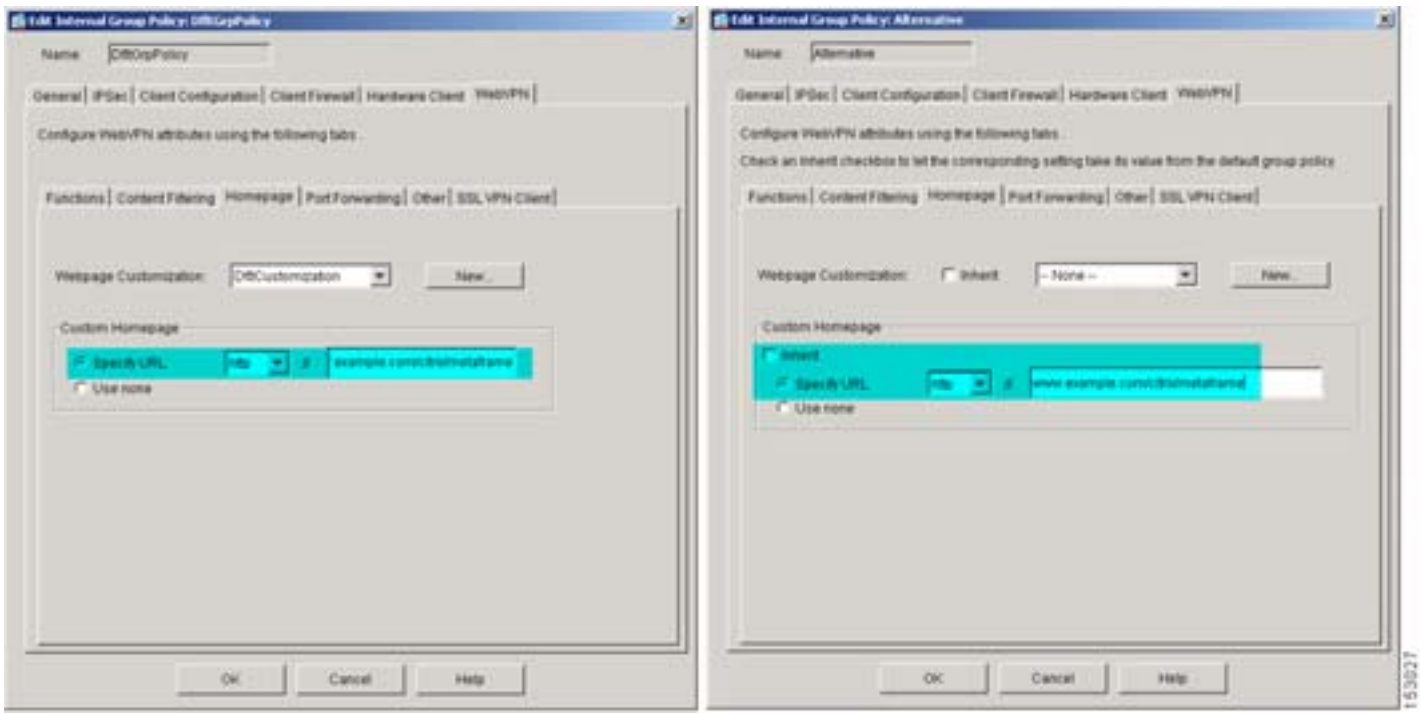
- 代替グループ ポリシーを設定して、WebVPN ホーム ページをリダイレクトする。

  デフォルトでは、ユーザは割り当てられたそれぞれのグループ ポリシーから Custom Homepage 設定を継承します。

  WebVPN ホーム ページをリダイレクトする内部または外部の各グループ ポリシーで、Group Policy テーブル内のポリシーをダブルクリックして、**WebVPN** > **Homepage** タブを開き、Custom Homepage 領域の **Inherit** をオフにしてから、**Specify URL** をオンにし、ドロップダウン メニューから **http** を選択し、右側のフィールドに Citrix サーバの URL を入力して、**OK** をクリックします。

図 7-14 は、DfltGrpPolicy と代替ポリシーの WebVPN > Homepage タブを比較しています。

図 7-14　DfltGrpPolicy と代替グループ ポリシーのホーム ページ リダイレクション



(注)　代替グループ ポリシーの Inherit チェックボックスをオンにすると、ポリシーはデフォルト グループ ポリシーの Custom Homepage 領域の設定を使用します。Inherit チェックボックスをオフにすると、代替グループ ポリシーの Custom Homepage 領域の設定をカスタマイズでき、デフォルト グループ ポリシーの設定に依存しなくなります。

ステップ 3　**Apply** をクリックして、変更したグループ ポリシーをフラッシュ デバイスに保存します。

ユーザ アカウントへのホーム ページのリダイレクト

WebVPN ホーム ページをグループ ポリシーにリダイレクトする代わりに、ユーザ アカウントにリダイレクトできます。ホーム ページをリダイレクトする各ユーザ アカウントに対して、次の手順を実行します。

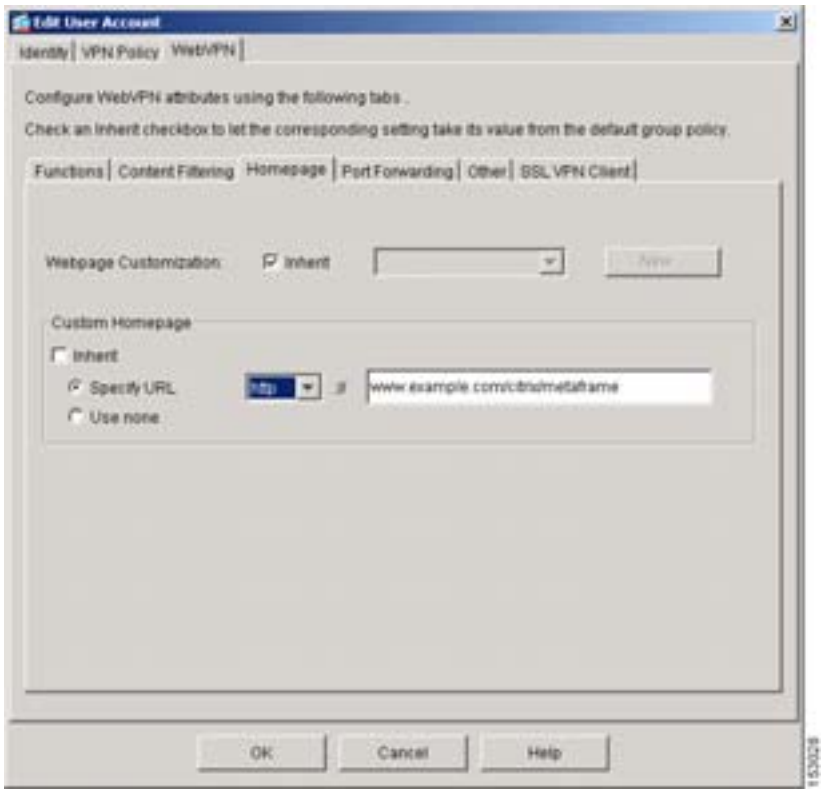
ステップ 1　Configuration > Properties > Device Administration > User Accounts を選択します。

User Accounts ウィンドウが開きます。

ステップ 2　ユーザ名をダブルクリックし、**WebVPN** > **Homepage** タブを開きます。

図 7-15 に、Edit User Account WebVPN > Homepage タブを示します。

図 7-15　Edit User Account WebVPN > Homepage タブ



ステップ 3　Custom Homepage 領域の **Inherit** チェックボックスをオフにして、**Specify URL** をオンにし、ドロップダウン メニューから **http** を選択してから、右側のフィールドに Citrix サーバの URL を入力して、**OK** をクリックします。

（注）　Inherit チェックボックスをオンにすると、ユーザ アカウントは、割り当てられたグループ ポリシーから Custom Homepage 設定を使用します。Inherit チェックボックスをオフにすると、そのユーザの設定をカスタマイズできます。

ステップ 4　**Apply** をクリックして、変更したユーザ アカウントをフラッシュ デバイスに保存します。

Citrix サーバへのリンクを WebVPN ホーム ページに追加する

WebVPN ユーザが Citrix サーバにアクセスできるようにするために、サーバへのリンクを WebVPN ホーム ページまたはフローティング ツールバーに表示できます（図 7-16）。

図 7-16　WebVPN ホーム ページおよびフローティング ツールバー

ユーザが実行する作業は、Web Bookmarks メニューの Citrix リンクまたは Citrix サーバにアクセスするためのリストをクリックするだけです。

Citrix サーバへのリンクを用意して、設定するためには、次の項の手順を使用します。

- URL リスト マッピングの確認（P.7-20）
- Citrix サーバへのリンクの設定（P.7-22）

URL リスト マッピングの確認

WebVPN ホーム ページに URL を挿入するには、1 つ以上の既存の URL リストを変更するか、新しいリストを 1 つ以上追加する必要があります（「リスト」に、1 つの URL だけを含めることができます）。

変更するリストを決めたり、新しいリストを追加するかどうかを判断したりするには、Citrix リンクを作成するグループ ポリーとユーザ アカウントがリストを使用しているかどうか、使用している場合はどのリストを使用しているかを確認する必要があります。現在のグループ ポリシーとユーザ アカウントの設定を確認し、処理方法を決定します。手順は次のとおりです。

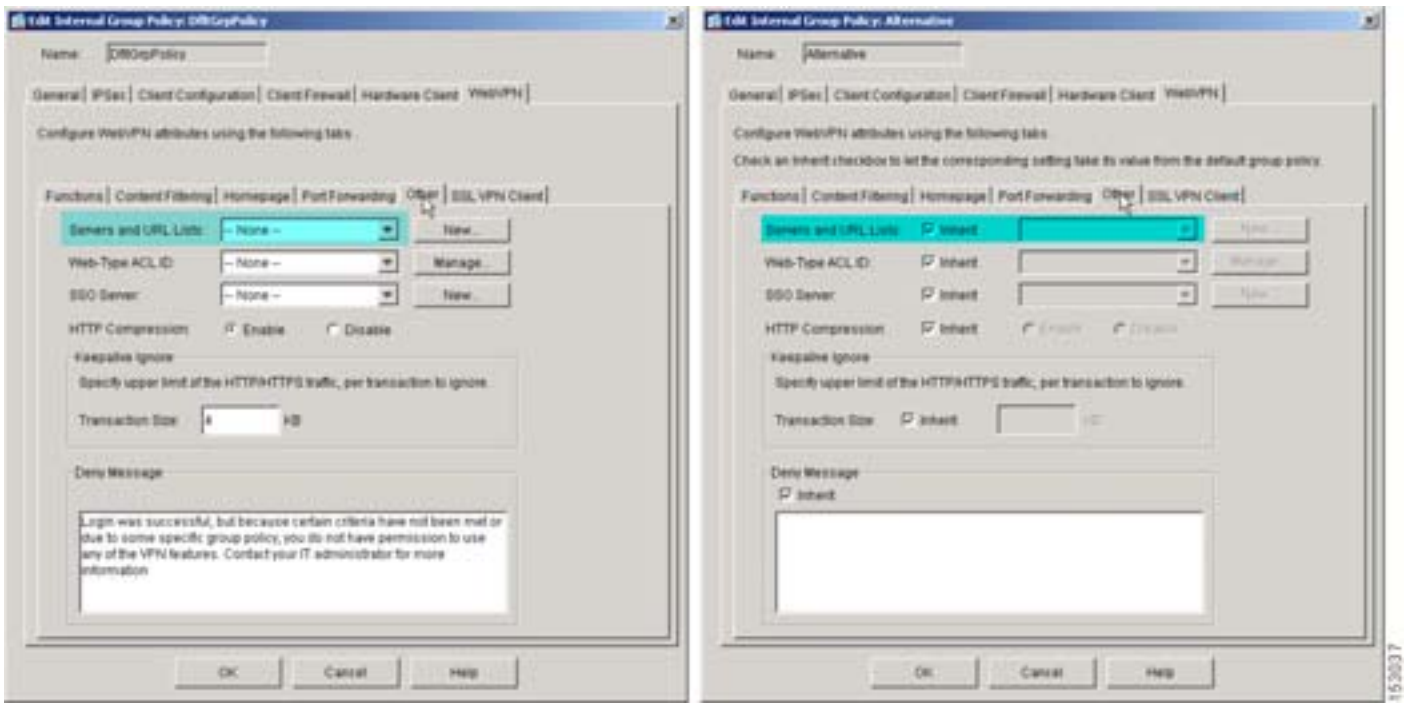
ステップ 1　Configuration > VPN > General > Group Policy を選択します。

Group Policy ウィンドウが開きます。

ステップ 2　各グループ ポリシーで、ポリシー名をダブルクリックし、**WebVPN** > **Other** タブを開きます。

図 7-17 は、デフォルト グループ ポリシーと代替ポリシーの WebVPN > Other タブを比較しています。

図 7-17　DfltGrpPolicy と代替グループ ポリシーの Servers and URL Lists



ステップ 3　Servers and URLs Lists アトリビュートの値を書き留めてから、**Cancel** をクリックします。

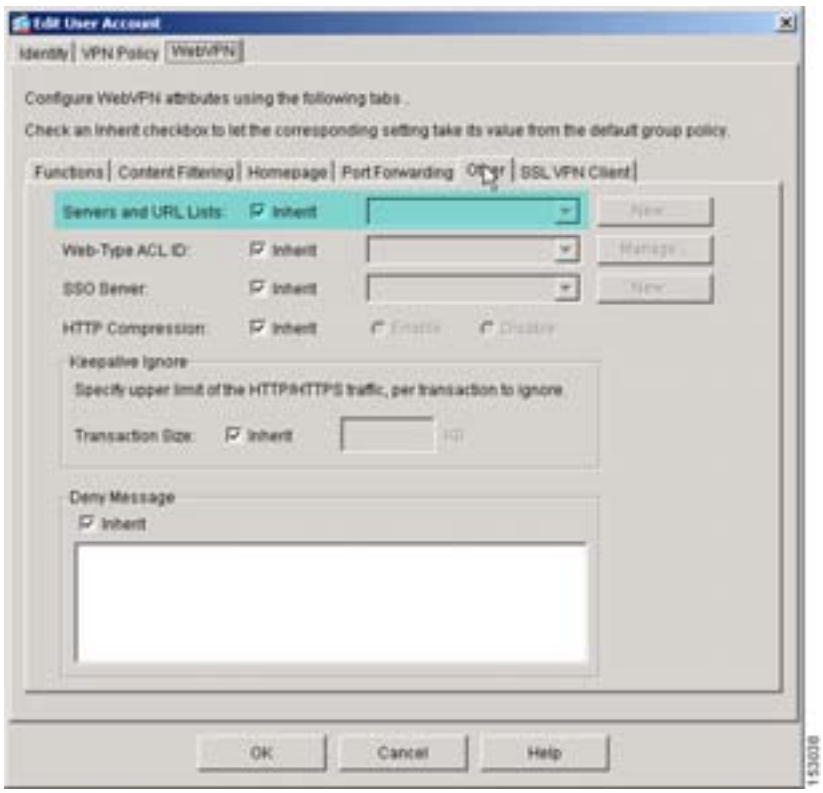
ステップ 4　Configuration > Properties > Device Administration > User Accounts を選択します。

User Accounts ウィンドウが開きます。

ステップ 5　Citrix サービスに対するサポートを追加する各ユーザ アカウントで、ポリシー名をダブルクリックして、**WebVPN** > **Other** タブを開きます。

図 7-18 に、ユーザ アカウント例の WebVPN > Other タブ上の Servers and URL Lists アトリビュートを示します。

図 7-18　ユーザ アカウントの Servers and URL Lists アトリビュート



ステップ 6　Servers and URLs Lists アトリビュートの値を書き留めてから、**Cancel** をクリックします。

Citrix サーバへのリンクの設定

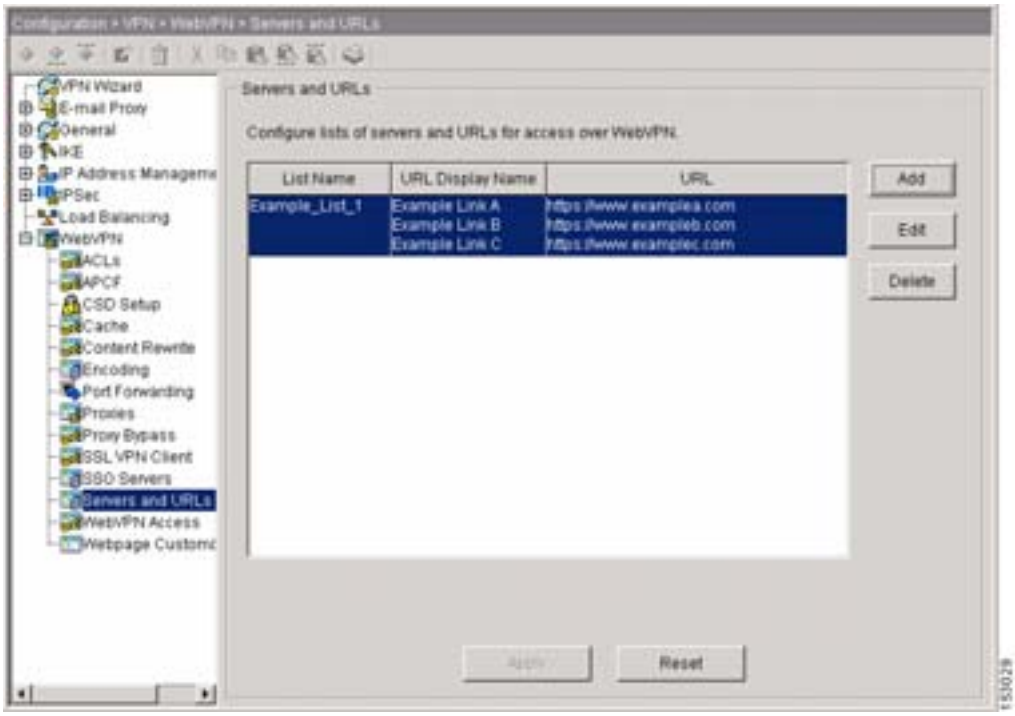
Citrix MetaFrame サービスを提供するグループ ポリシーとユーザが URL リストを使用しているかどうかを確認し、使用している場合はその URL リストの名前を確認できたので、サーバと URL のセキュリティ アプライアンス設定を変更して、Citrix サーバへのリンクを作成できます。

Citrix サーバへのリンクを作成し、Citrix アクセスを設定するグループ ポリシーとユーザに割り当てる手順は、次のとおりです。

ステップ 1　Configuration > VPN > WebVPN > Servers and URLs を選択します。

Servers and URLs ウィンドウが開きます（図 7-19）。

図 7-19　Servers and URLs



このウィンドウに表示される各リストは、リンク名（URL Display Name）と、それらに関連付けられた URL で構成されます。新しいリストを設定したら、最低 1 つのグループ ポリシーまたはユーザ アカウントに割り当てて、WebVPN ホーム ページとフローティング ツールバーにリストを表示します。

グループ ポリシーまたはユーザ アカウントにすでに割り当てられているリストにリンクを追加すると、WebVPN ホーム ページとフローティング ツールバーは、後続の各ログインでリンクを自動的に追加します。

（注） Servers and URLs リストには、デフォルト グループ ポリシーの場合は 1 対 1 のアソシエーション、代替グループ ポリシーとユーザ アカウントの場合は 1 対多の関係があります。1 つのリストを複数のグループ ポリシーとユーザ アカウントに割り当てることができますが、複数のリストを同一のグループ ポリシーまたはユーザ アカウントに割り当てることはできません。

ステップ 2　次のどれかの項の手順を続けます。

- Citrix サービスを設定するグループ ポリシーまたはユーザ アカウントに Servers and URLs リストが割り当てられていない場合は、P.7-24 の「Servers and URLs リストの追加」を参照してください。
- Citrix サービスを設定するグループ ポリシーまたはユーザ アカウントに Servers and URLs リストがすでに割り当てられている場合は、P.7-25 の「Servers and URLs リストへの URL の追加」を参照してください。

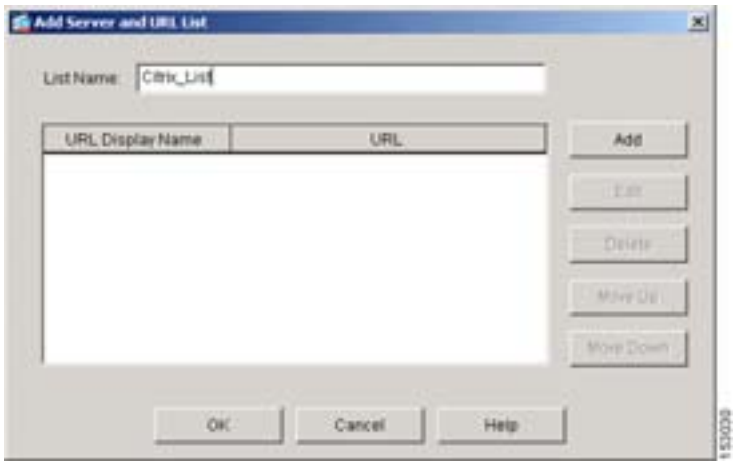
Servers and URLs リストの追加

Citrix MetaFrame サービスへのアクセスを設定するグループ プロファイルまたはユーザ アカウントに Servers and URLs リストが割り当てられていない場合は、前の項の手順から継続して、Servers and URLs リストを追加します。

ステップ 1　図 7-19 に示すように、Servers and URLs ウィンドウの Add をクリックします。

Add Server and URL List ウィンドウが開きます（図 7-20）。

図 7-20　Add Server and URL List

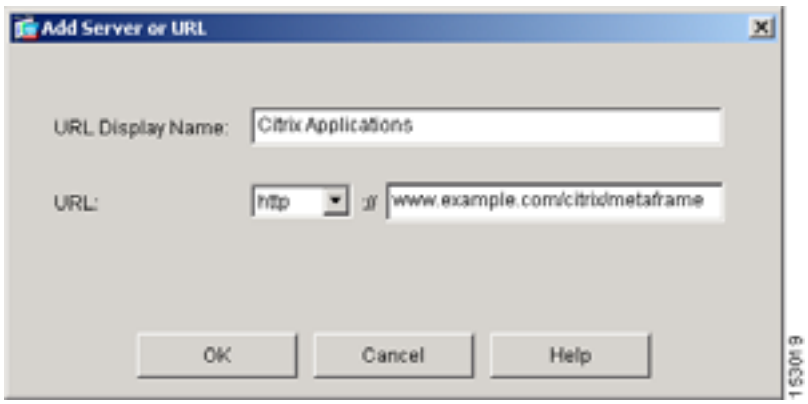


ステップ 2　List Name フィールドに名前を入力して、Servers and URLs の他の設定とこのリストとを区別します。使用するグループ プロファイルとユーザ アカウントを説明する名前を付けることを推奨します。

ステップ 3　**Add** をクリックして、Citrix リンクを作成します。

Add Server or URL ウィンドウが開きます（図 7-21）。

図 7-21　Add Server or URL



ステップ 4　ドロップダウン メニューから **http** を選択し、右側のフィールドに Citrix サーバの URL を入力して、**OK** をクリックします。

図 7-20 に示すように、ASDM は Add Server and URL List テーブルに URL エントリを挿入します。

ステップ 5　**OK** をクリックします。

図 7-19 に示すように、ASDM は Servers and URLs ウィンドウにリスト エントリを挿入します。

ステップ 6　**Apply** をクリックして、変更した Servers and URLs 設定をフラッシュ デバイスに保存します。

ステップ 7　Configuration > VPN > General > Group Policy を選択します。

Group Policy ウィンドウが開きます。

ステップ 8　Citrix MetaFrame サーバに URL を提供する各グループ ポリシーで、グループ ポリシーをダブルクリックして、**WebVPN** > **Other** タブを開き、グループ ポリシーがデフォルト グループ ポリシーの代替である場合は、Servers and URL Lists の隣にある **Inherit** チェックボックスをオフにし、作成したリストを Servers and URL Lists アトリビュートの右側にあるドロップダウン メニューで選択して、**OK** をクリックします。

ステップ 9　**Apply** をクリックして、変更したグループ ポリシーをフラッシュ デバイスに保存します。

ステップ 10　Configuration > Properties > Device Administration > User Accounts を選択します。

User Accounts ウィンドウが開きます。

ステップ 11　Citrix MetaFrame サーバに URL を提供する各カスタム ユーザ アカウントで、ユーザ アカウントをダブルクリックして、**WebVPN** > **Other** タブを開き、Servers and URL Lists アトリビュートの隣にある **Inherit** チェックボックスをオフにし、作成したリストを Servers and URL Lists の右側にあるドロップダウン メニューで選択して、**OK** をクリックします。

ステップ 12　**Apply** をクリックして、変更したユーザ アカウントをフラッシュ デバイスに保存します。

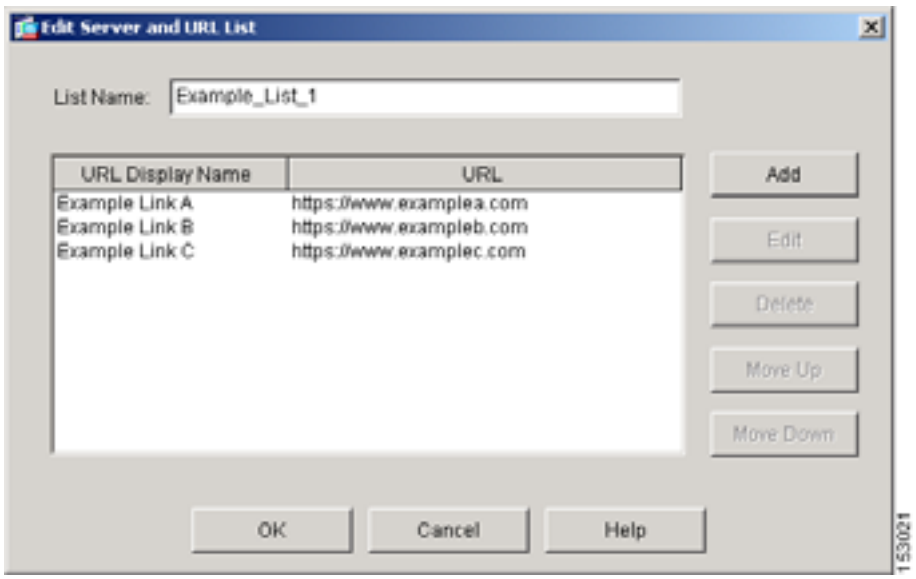
Servers and URLs リストへの URL の追加

図 7-19 に表示された Servers and URLs テーブル内のエントリを変更する手順を続けます。この項の手順は、Citrix サーバへの URL を追加するグループ ポリシーまたはユーザ アカウントにすでに Servers and URLs リストが割り当てられている場合にだけ使用します。

ステップ 1　Servers and URLs ウィンドウのエントリをダブルクリックします（図 7-19）。

Edit Server and URL List ウィンドウが開きます（図 7-22）。

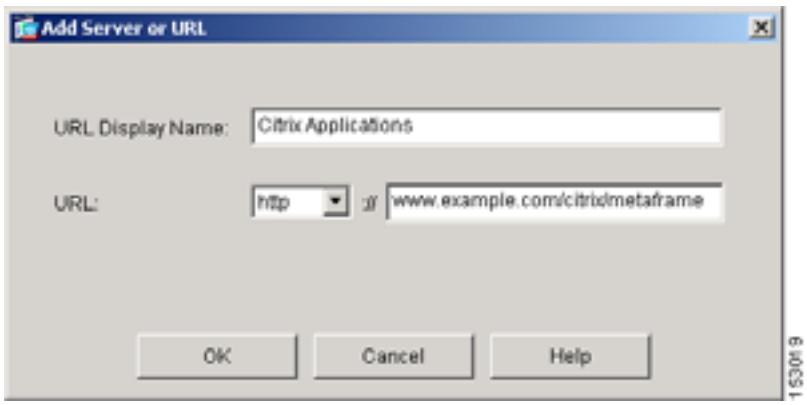
図 7-22　Edit Server and URL List



ステップ 2　**Add** をクリックして、このリストに Citrix リンクを挿入します。

Add Server or URL ウィンドウが開きます（図 7-23）。

図 7-23　Add Server or URL



ステップ 3　ドロップダウン メニューから **http** を選択し、右側のフィールドに Citrix サーバの URL を入力して、**OK** をクリックします。

図 7-22 に示すように、ASDM は Edit Server and URL List テーブルに URL エントリを挿入します。

ステップ 4　**OK** をクリックします。

図 7-19 に示すように、ASDM は Servers and URLs ウィンドウにリスト エントリを挿入します。

ステップ 5　**Apply** をクリックして、変更したリストをフラッシュ デバイスに保存します。

(注) Citrix　サーバへのリンクを追加するすべてのグループ　ポリシーとユーザ　アカウントに Servers and URLs リストがすでに割り当てられている場合は、このステップで Citrix サーバへのリンクの設定が完了します。そうでない場合は、これ以降の手順を続けます。

ステップ 6　Configuration > VPN > General > Group Policy を選択します。

Group Policy ウィンドウが開きます。

ステップ 7　新しく追加した Citrix サーバへのリンクを含むリストを割り当てる各グループ ポリシーで、グループ ポリシーをダブルクリックして、**WebVPN** > **Other** タブを開き、グループ ポリシーがデフォルト グループ ポリシーの代替である場合は、Servers and URL Lists の隣にある **Inherit** チェックボックスをオフにし、作成したリストを Servers and URL Lists の右側にあるドロップダウン メニューで選択して、**OK** をクリックします。

ステップ 8　**Apply** をクリックして、変更したグループ ポリシーをフラッシュ デバイスに保存します。

ステップ 9　Configuration > Properties > Device Administration > User Accounts を選択します。

User Accounts ウィンドウが開きます。

ステップ 10　新しく追加した Citrix サーバへのリンクを含むリストを割り当てる各カスタム ユーザ アカウントで、ユーザ アカウントをダブルクリックして、**WebVPN** > **Other** タブを開き、Servers and URL Lists の隣にある **Inherit** チェックボックスをオフにし、作成したリストを Servers and URL Lists の右側にあるドロップダウン メニューで選択して、**OK** をクリックします。

ステップ 11　**Apply** をクリックして、変更したユーザ アカウントをフラッシュ デバイスに保存します。

WebVPN ホーム ページでの URL エントリのイネーブル化

Citrix サーバに WebVPN ユーザがアクセスできるようにするために、URL エントリをイネーブルにして、サーバにアクセスするために入力する URL をユーザに送信できます。ユーザは WebVPN ホーム ページまたはフローティング ツールバーの Enter Web Address フィールドに URL を入力します（図 7-16）。

デフォルト グループ ポリシーの Enable URL Entry アトリビュートのデフォルト設定は、オンです。

グループ ポリシーまたはユーザ アカウントの WebVPN > Functions タブの Enable URL Entry アトリビュートをオンにした場合、リモート ユーザは、WebVPN ホーム ページまたはフローティング ツールバーに Citrix サーバの URL を入力できます。デフォルトでは、図 7-11 の左側に示すように、Enable URL Entry アトリビュートがデフォルトのグループ ポリシーでオンになっています。代替グループ ポリシーまたはユーザ アカウントで Inherit をオフにすると、ASDM は自動的にチェック マークを挿入してこのパラメータをイネーブルにします。ユーザが Citrix サーバの URL を含む URL を入力できるようにするには、デフォルト設定（オン）を使用します。それ以外の場合は、このアトリビュートをオフにします。

デフォルトで Enable URL Entry アトリビュートがイネーブルにされているため、WebVPN ホーム ページまたはフローティング ツールバーに Enter Web Address フィールドを表示するための作業が必要になる可能性はほとんどありません。ただし、ユーザが Enter Web Address フィールドを確実に

使用できるように、各グループ ポリシーとユーザ アカウントでこのアトリビュートの値がオンになっていることを確認することを推奨します。Enable URL Entry アトリビュートがオンになっているか、適用可能なそれぞれのグループ ポリシーまたはユーザ アカウントから継承されているかを確認する手順は、次のとおりです。

ステップ 1　Citrix MetaFrame サービスをイネーブルにした各グループ ポリシーで、Configuration > VPN > General > Group Policy を選択し、Group Policy テーブル内のエントリをダブルクリックして（Citrix アクセスを使用している場合は DfltGrpPolicy から開始）、**WebVPN** > **Functions** タブを開き、**Inherit** または **Enable URL Entry** および **Enable Citrix MetaFrame** の両方をオンにし、**OK** をクリックして、**Apply** をクリックします。

ステップ 2　Citrix MetaFrame サービスをイネーブルにした各ユーザ アカウントで、Configuration > Properties > Device Administration > User Accounts を選択し、User Accounts テーブル内のエントリをダブルクリックして、**WebVPN** > **Functions** タブを開き、**Inherit** または **Enable URL Entry** および **Enable Citrix MetaFrame** の両方をオンにし、**OK** をクリックして、**Apply** をクリックします。

WebVPN に対する SSO の設定

この章では、WebVPN ユーザに対する Single Sign-on（SSO; シングル サインオン）の設定例を示します。この章には、次の項があります。

WebVPN での SSO の使用

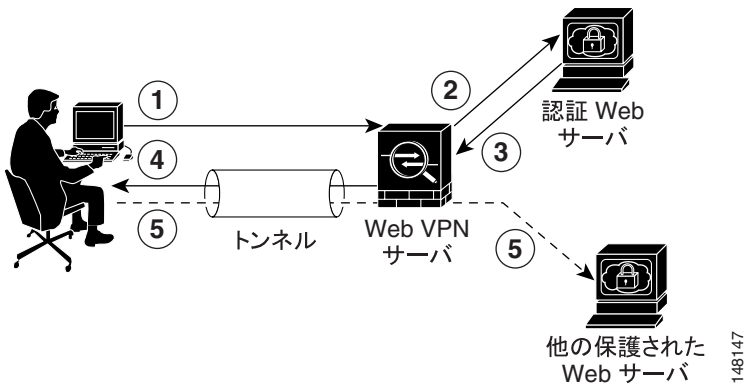
SSO では、WebVPN ユーザがユーザ名とパスワードを 1 回入力するだけで、保護された複数のサービスと Web サーバにアクセスできます。一般に、SSO のメカニズムは、AAA プロセスの一部として開始されるか、AAA サーバのユーザ認証に成功した直後に開始されます。セキュリティ アプライアンスで実行する WebVPN サーバは、認証サーバに対するユーザのプロキシとして動作します。ユーザがログインすると、WebVPN サーバは、ユーザ名とパスワードを含む SSO 認証要求を HTTPS を使用して認証サーバに送信します。サーバが認証要求を受け入れた場合は、WebVPN サーバに SSO 認証クッキーを返信します。セキュリティ アプライアンスは、ユーザに代わってこのクッキーを保持し、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。

WebVPN は 3 つの SSO 認証方式をサポートしており、2 つの方式を ASDM で設定できます。これら 2 つの方式は、Computer Associates の eTrust SiteMinder サーバ（以前の名称は Netegrity SiteMinder）による SSO と、HTTP Form プロトコルによる SSO です。3 つ目の方式である、HTTP Basic と NTLMv1（NT LAN Manager）認証による SSO は、現在 セキュリティ アプライアンス コマンドライン インターフェイスを使用した場合にだけ設定できます。

図 8-1 に、3 つすべての方式で使用される次の主な SSO 認証手順を示します。

1. 最初に、WebVPN ユーザは、ユーザ名とパスワードを入力して、セキュリティ アプライアンス上の WebVPN サーバにログインします。
2. ユーザのプロキシとして動作する WebVPN サーバは、このフォーム データ（ユーザ名とパスワード）を、認証 Web サーバに転送します。
3. 認証 Web サーバがユーザのデータを承認した場合は、ユーザの代行で保管していた認証クッキーを WebVPN サーバに戻します。
4. WebVPN サーバはユーザまでのトンネル接続を確立します。
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 8-1　HTTP Form による SSO 認証



SiteMinder による SSO 認証の設定

この項では、SiteMinder を使用して SSO をサポートするためのセキュリティ アプライアンスの設定方法を説明します。ユーザの Web サイトのセキュリティ インフラストラクチャにすでに SiteMinder が組み込まれている場合、通常は SiteMinder による SSO の実装を選択します。この方式により、SSO 認証は AAA から切り離され、AAA プロセスが完了すると、この認証が 1 回実施されます。WebVPN ユーザまたはグループに SSO を設定する場合は、まず RADIUS サーバまたは LDAP サーバなどの AAA サーバを設定する必要があります。その後で、WebVPN の SSO サポートをセットアップできます。

この項は、次の内容で構成されています。

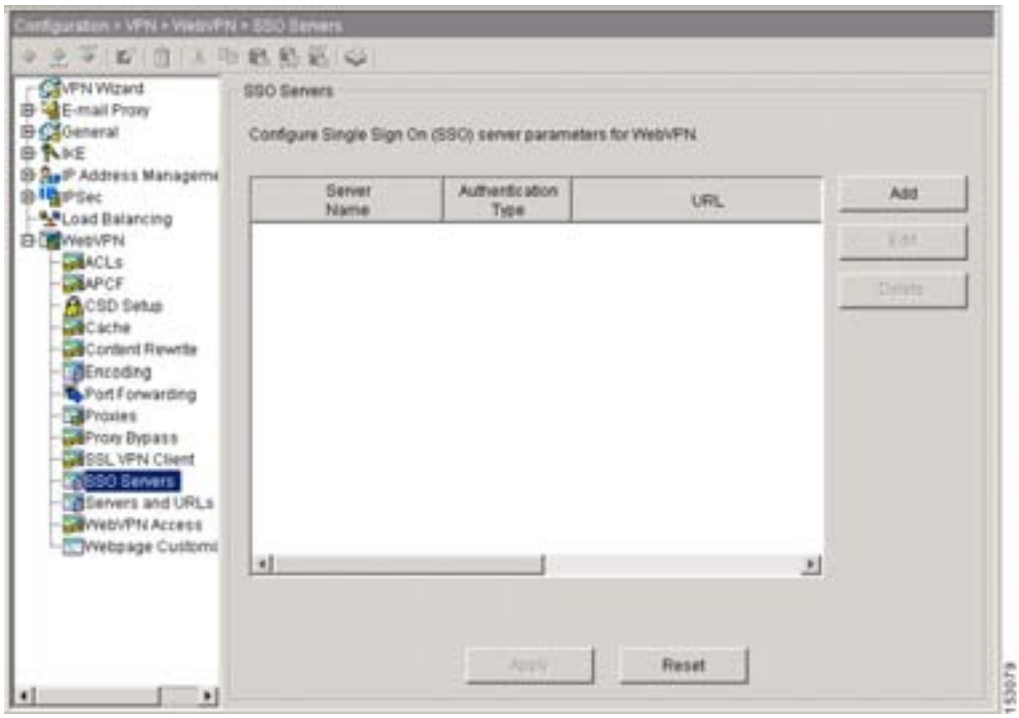
SiteMinder に対するセキュリティ アプライアンスの設定

新しい SiteMinder サーバを使用して SSO を設定するには、次の手順を実行します。

ステップ 1　Cisco ASDM メイン ウィンドウで、**Configuration > VPN > WebVPN > SSO Servers** を選択します。

図 8-2 のように、ウィンドウの右側に SSO Servers 領域が表示されます。

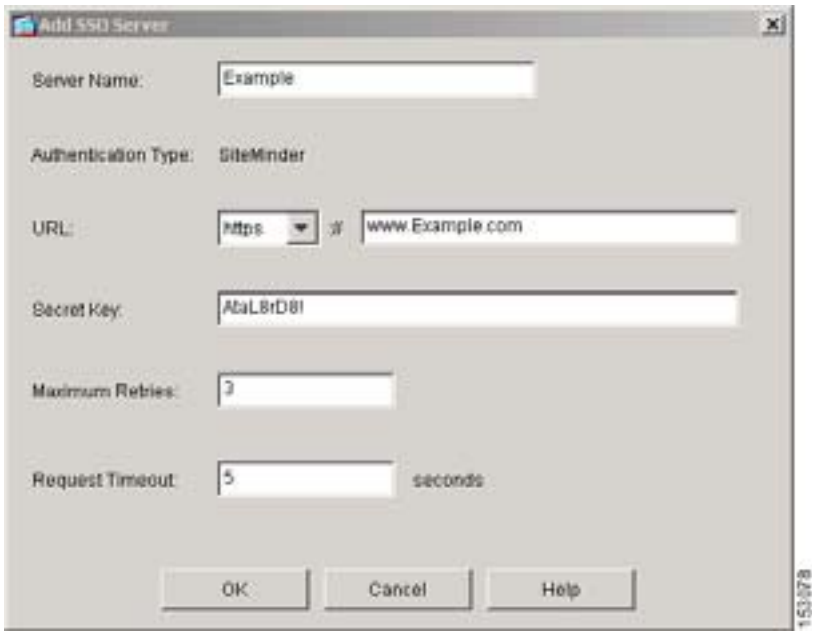
図 8-2　SSO Servers 領域が表示された ASDM ウィンドウ



ステップ 2　SSO Servers 領域で **Add** をクリックします。

図 8-3 のように、Add SSO Server ダイアログボックスが表示されます。

図 8-3　Add SSO Server ダイアログボックス



ステップ 3　Server Name フィールドに、SiteMinder SSO サーバの名前を入力します。

入力できる文字の範囲は、4 ～ 31 文字です。

この例では、サーバ名は *Example* です。

ステップ 4　次の手順を実行して、SSO サーバの URL を入力します。

a.　メニューから **HTTP** または **HTTPS** を選択します。

この例では、HTTPS を選択して、セキュリティ アプライアンスと SiteMinder サーバ間の認証メッセージを保護します。

b.　サーバ URL の後の部分を入力します。

この例では、URL の後の部分は *www.Example.com* です。

これは、セキュリティ アプライアンスが SSO 認証要求を行う SSO サーバの URL です。

ステップ 5　Secret Key フィールドに秘密鍵を入力します。

これは、SSO サーバとの認証通信の暗号化に使用されます。鍵は、任意の標準またはシフト式英数字で構成されます。文字数の制限はありません。

秘密鍵はパスワードに類似しており、作成し、保存してから、セキュリティ アプライアンスと SiteMinder Policy Server の両方に入力します。P.8-10 の「SiteMinder へのシスコの認証スキームの追加」を参照してください。

この例では、秘密鍵は AtaL8rD8! です。

ステップ 6　Maximum Retries フィールドに、SSO 認証が失敗した場合にセキュリティ アプライアンスがリトライする回数を入力します。このステップはオプションです。

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。

この例では、最大のリトライ数は 3 回です。

ステップ 7　Request Timeout フィールドに、失敗した SSO 認証がタイムアウトするまでの秒数を入力します。このステップはオプションです。

範囲は 1 ～ 30 秒で、デフォルトは 5 秒です。

この例では、タイムアウトが 5 秒後に行われます。

ステップ 8　**OK** をクリックして、ASDM ウィンドウの SSO Server テーブルにこの新しい SSO サーバを入力します。

ステップ 9　**Apply** をクリックして、新しい SSO サーバをセキュリティ アプライアンスの実行コンフィギュレーションに追加します。

グループ ポリシーとユーザへの SSO サーバの割り当て

SSO サーバの設定が完了したら、次はグループ ポリシーまたはユーザに SSO 認証を指定する必要があります。この項の内容は、次のとおりです。

グループ ポリシーへの SSO サーバの割り当て

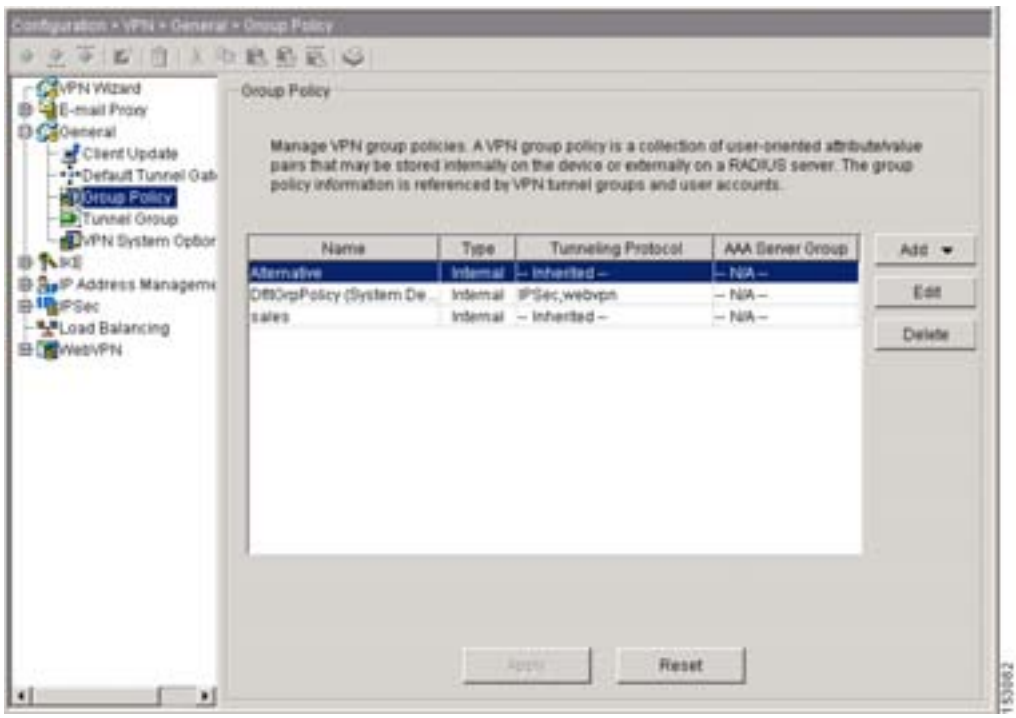
（注）　グループ　ポリシーを設定する総合的な手順は、このマニュアルの他の部分で提供します。次の手順は、SiteMinder SSO サーバを設定する場合にだけ適用されます。

グループ ポリシーに SSO サーバを割り当てるには、次の手順を実行します。

ステップ 1　Cisco ASDM メイン ウィンドウで、**Configuration > VPN > General > Group Policy** を選択します。

図 8-4 のように、ウィンドウに Group Policy 領域が表示されます。

図 8-4　Group Policy 領域が表示された ASDM ウィンドウ

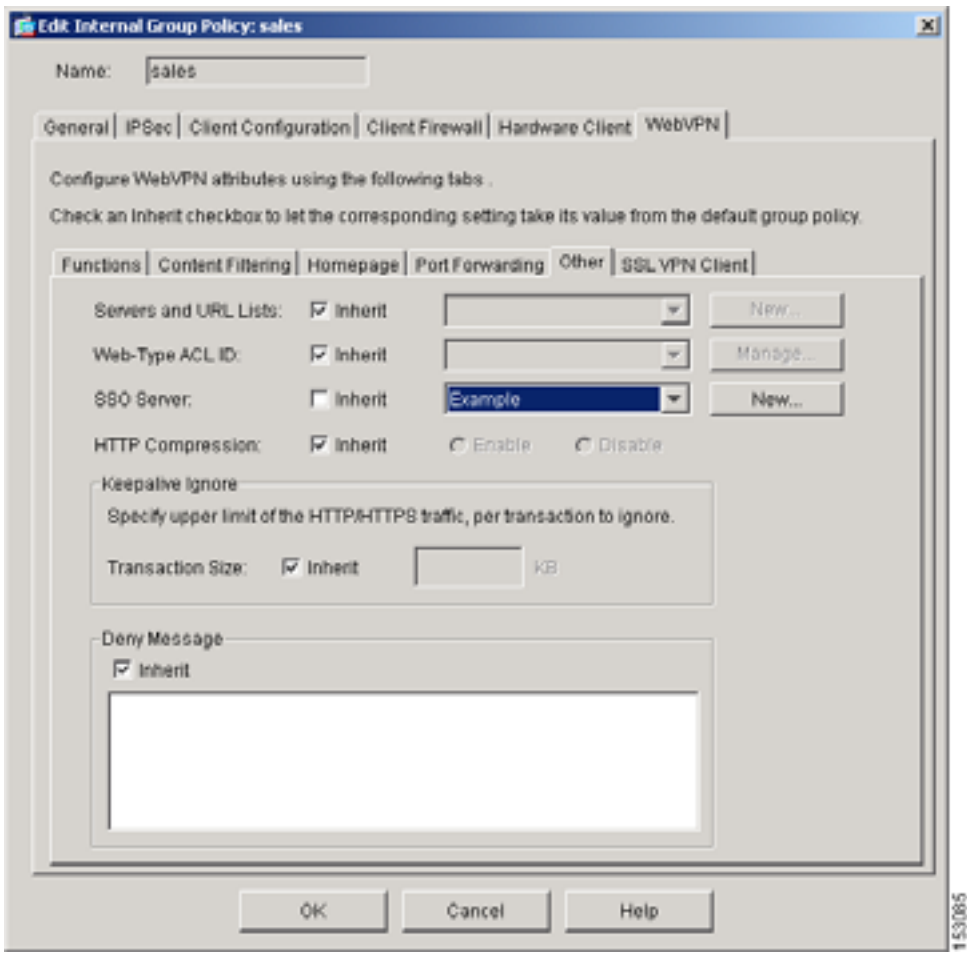


ステップ 2　Group Policy テーブルで、SiteMinder SSO サーバを割り当てるグループ ポリシーをクリックします。

ステップ 3　**Edit** をクリックします。

図 8-5 のように、Edit Internal Group Policy ダイアログボックスが表示されます。

図 8-5　Edit Internal Group Policy ダイアログボックス



ステップ 4　**General** タブをクリックしてから、General タブの **Other** タブをクリックします。

ステップ 5　SSO Server の隣で、次の内容を実行します。

- SSO Server の **Inherit** チェックボックスをオフにします。
- メニューから新しい SSO サーバを選択します。
  この例では、SSO サーバは Example という名前です。

ステップ 6　**OK** をクリックして、ASDM ウィンドウに戻ります。

ステップ 7　**Apply** をクリックして、割り当てをセキュリティ アプライアンスの実行コンフィギュレーションに入力します。

ユーザへの SSO サーバの割り当て

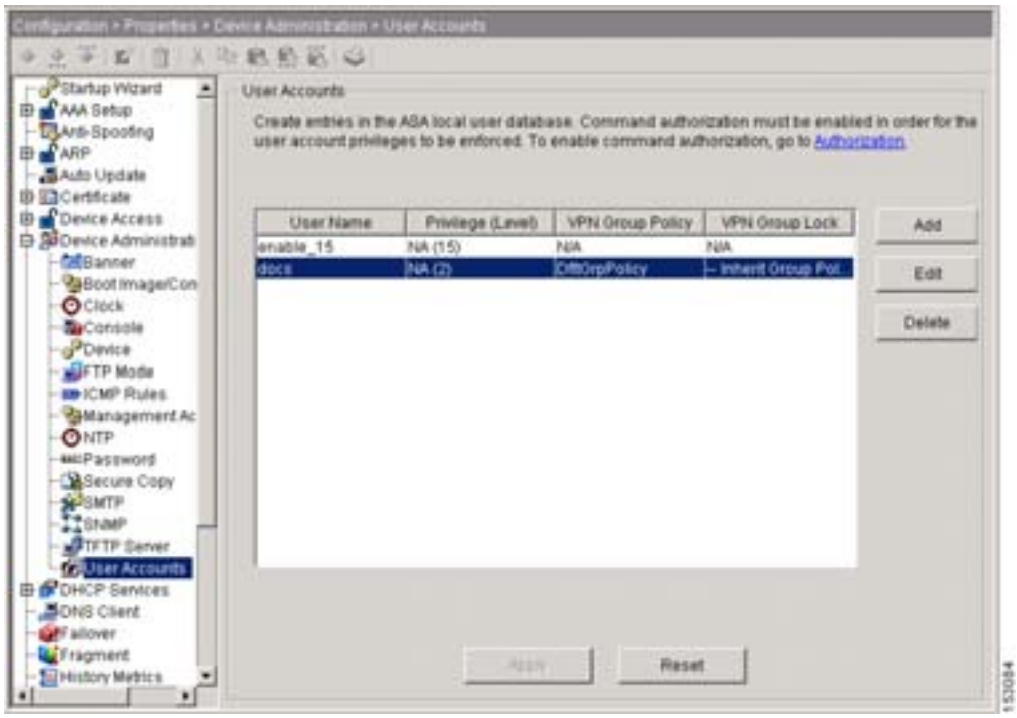
（注） ユーザを設定する総合的な手順は、このマニュアルの他の部分で提供します。次の手順は、SiteMinder SSO サーバを設定する場合にだけ適用されます。

次の手順を実行して、ユーザに SSO サーバを割り当てることもできます。

ステップ 1　Cisco ASDM メイン ウィンドウで、**Configuration > Properties > Device Administration > Users** を選択します。

図 8-6 のように、ウィンドウに User Accounts 領域が表示されます。

図 8-6　User Accounts 領域が表示された ASDM ウィンドウ

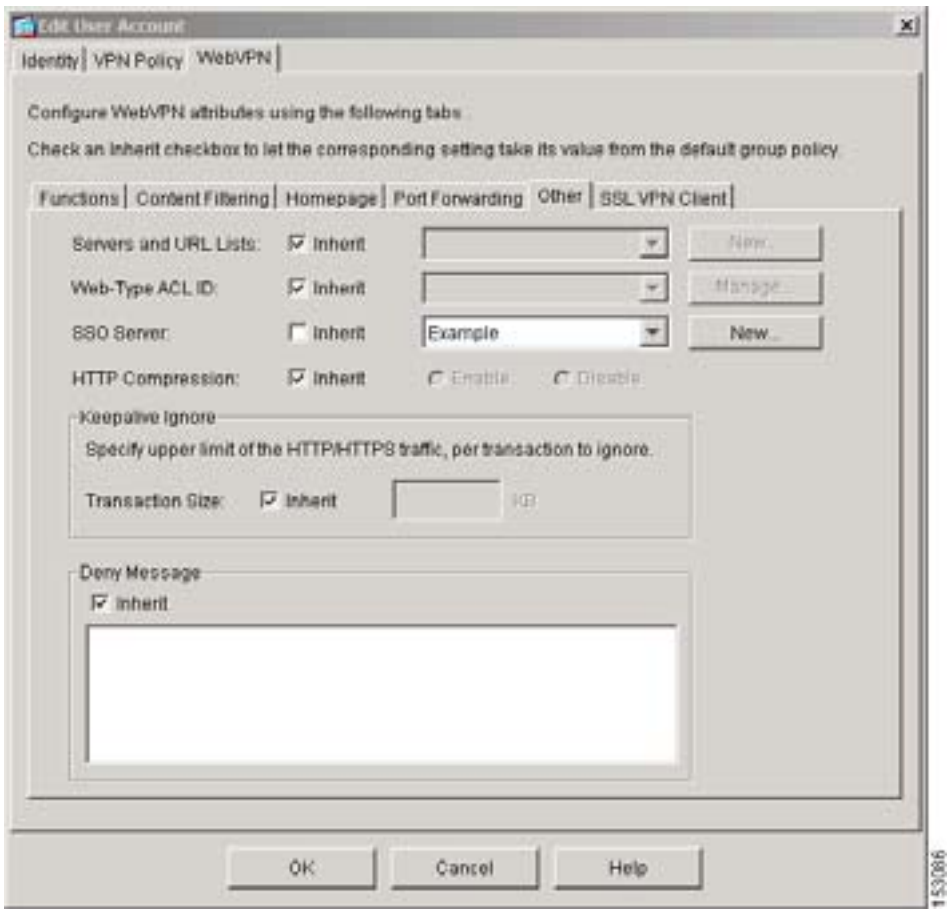


ステップ 2　User Accounts テーブルから、SiteMinder SSO サーバを割り当てる User Name をクリックします。

ステップ 3　**Add** をクリックします。

図 8-7 のように、Edit User Account ダイアログボックスが表示されます。

図 8-7　Edit User Account ダイアログボックス



ステップ 4　**WebVPN** タブをクリックしてから、WebVPN タブの **Other** タブをクリックします。

ステップ 5　SSO Server の隣で、次の内容を実行します。

- SSO Server の **Inherit** チェックボックスをオフにします。
- メニューから新しい SSO サーバを選択します。
  この例では、SSO サーバは図 8-7 に示すように Example という名前です。

ステップ 6　**OK** をクリックして、ASDM ウィンドウに戻ります。

ステップ 7　**Apply** をクリックして、割り当てをセキュリティ アプライアンスの実行コンフィギュレーションに入力します。

SiteMinder へのシスコの認証スキームの追加

SiteMinder による SSO 用にセキュリティ アプライアンスを設定することに加えて、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 Computer Associates SiteMinder Policy Server を設定する必要があります。

(注)
- SiteMinder Policy Server の設定には、SiteMinder の使用経験が必要です。
- 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。
- 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 Policy Server にシスコの認証スキームを設定するには、次のタスクを実行します。

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、セキュリティ アプライアンスに設定したものと同じ秘密鍵を入力します。コマンドライン インターフェイスから **policy-server-secret** コマンドを入力するか、ASDM の Add SSO Server ダイアログボックスの Secret Key フィールドに入力するかのいずれかの方法でセキュリティ アプライアンスにこれを設定します。
- Parameter フィールドに、**CiscoAuthAPI** と入力します。

ステップ 2　CD から **cisco_vpn_auth.jar** ファイルを 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。

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 プロトコルの使用方法を説明します。HTTP Form プロトコルは SSO 認証を実行するための一般的な手段で、AAA 方式としても使用できます。このプロトコルは、WebVPN ユーザと認証 Web サーバとの間で認証情報を交換するセキュアな方式を提供します。HTTP Form は一般的なプロトコルとして、Web サーバや Web ベースの SSO 製品との高度な互換性を持ち、RADIUS サーバや LDAP サーバなど他の AAA サーバと共に使用することができます。

SiteMinder を使用する場合、セキュリティ アプライアンスは、認証 Web サーバに対する WebVPN ユーザのプロキシとして動作しますが、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セキュリティ アプライアンスを設定する必要があります。

(注)　HTTP Form プロトコルを使用して SSO を正しく設定するには、認証および HTTP プロトコル交換に関する実用的な知識が必要です。

セキュリティ アプライアンス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するフォーム パラメータを設定するときに、Web サーバが追加的に要求する非表示パラメータの中には、ユーザ側で当初認識できないものがある場合があります。認証アプリケーションによっては、ユーザ側に表示されず、ユーザが入力しない非表示データを要求する場合があります。しかし、認証 Web サーバが要求する非表示パラメータを見つけることは可能です。これは、セキュリティ アプライアンス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した場合は、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。非表示パラメータが必須かオプションかについてはヘッダー アナライザでは確認できないため、必須であることが判別できるまではすべての非表示パラメータを含めることを推奨します。

この項の内容は、次のとおりです。

HTTP Form データの収集

この項では、データが不明である場合に SSO を設定するために必要な HTTP Form データを検出および収集する手順を示します。このデータを収集するには、HTTP ヘッダー アナライザを使用して認証 Web サーバからの応答を分析する必要があります。

パラメータ データを収集するには、次の手順を実行します。

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、セキュリティ アプライアンスを経由せずに Web サーバのログイン ページに直接接続します。

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ます。

ステップ 2　HTTP ヘッダー アナライザでログイン交換を検証します。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 をコピーします。これは、Start URL です。

ステップ 3　Web サーバにログインするためのユーザ名とパスワードを入力して、**Enter** キーを押します。

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 アナライザで生成されます。

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-ac0
5-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFb
IrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2F
myemco%2F HTTP/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 を入力します。これは、後で action-uri パラメータを設定する際に必要になります。

ステップ 5　POST 要求の本文を検証して、次の内容をコピーします。

a.　ユーザ名パラメータ

この例では、このパラメータは userid です（値 anyuser ではありません）。

b.　パスワード パラメータ

この例では、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。この例では、非表示パラメータは、SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0 です。

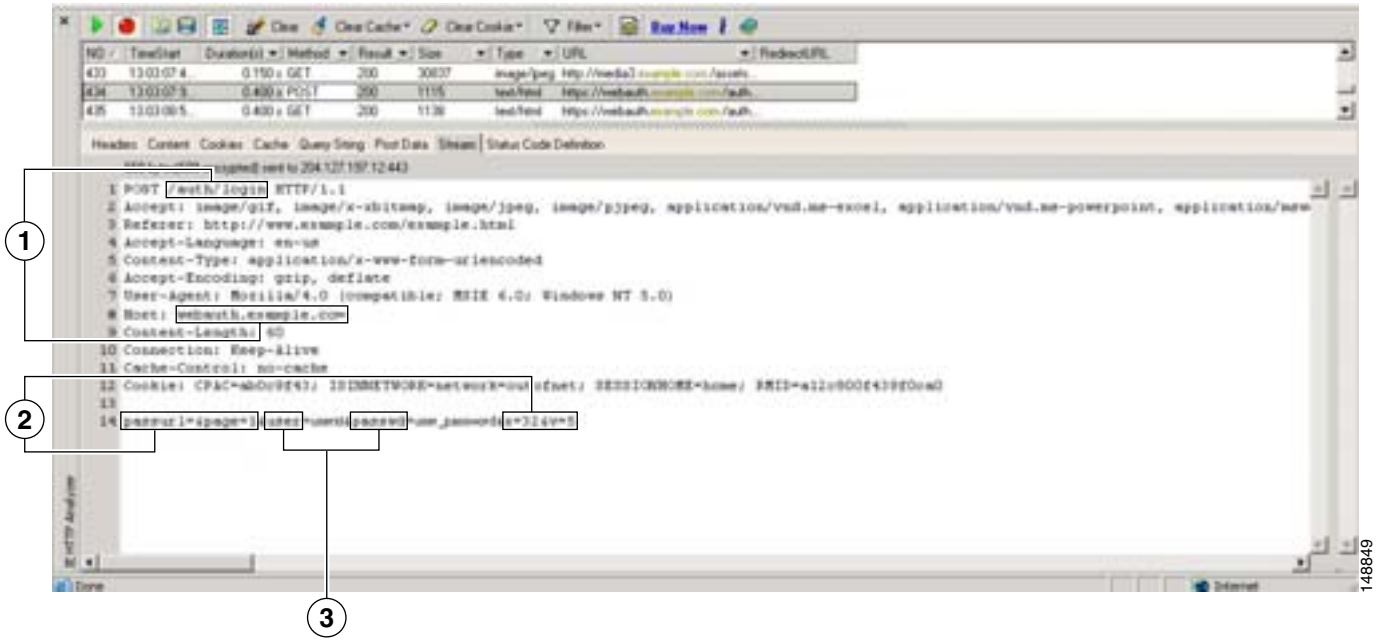
非表示パラメータは、一般的に次の形式で表されます。

```
<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した場合は、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。非表示パラメータが必須かオプションかについてはヘッダー アナライザでは確認できないため、必須であることが判別できるまではすべての非表示パラメータを含めることを推奨します。

図 8-8 に、HTTP ヘッダー アナライザの出力例に表示される action URI、非表示、ユーザ名、およびパスワードのパラメータを示します。これは一例です。出力内容は Web サイトによって大幅に異なることがあります。

図 8-8　action-uri、非表示、ユーザ名、およびパスワードのパラメータ



1	action URI パラメータ
2	非表示パラメータ
3	ユーザ名パラメータとパスワード パラメータ

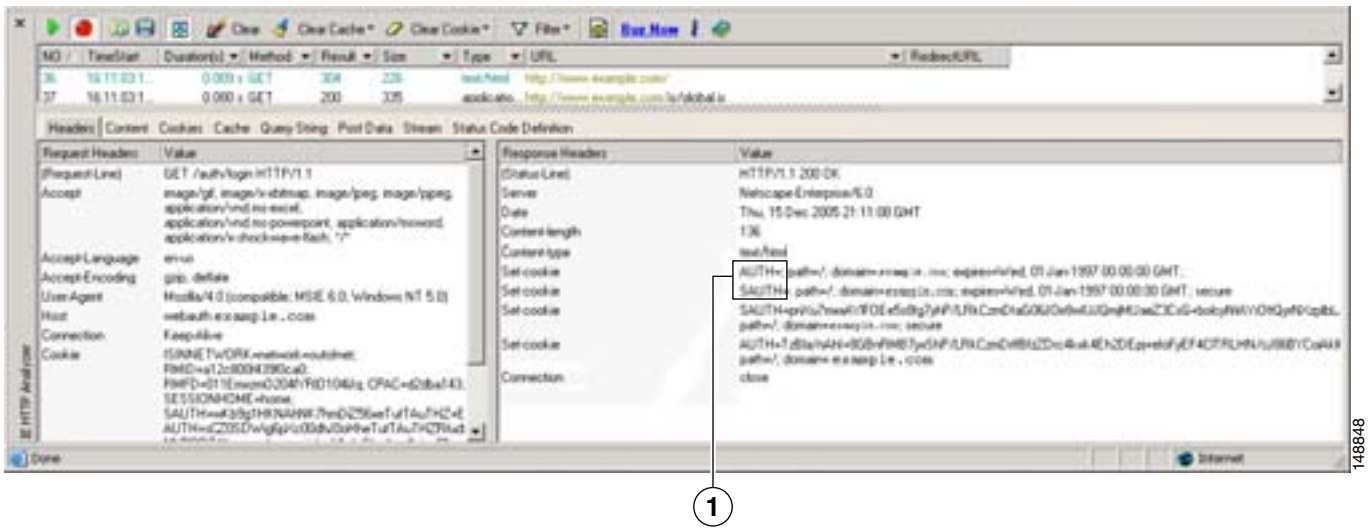
ステップ 6　Web サーバへのログインが成功したら、HTTP ヘッダー アナライザを使用して、サーバからユーザのブラウザ内に設定されているセッションのクッキー名を見つけることによって、サーバの応答を検証します。これは、Authentication Cookie Name 値です。

次のサーバ応答ヘッダーでは、セッションのクッキーの名前は SMSESSION です。必要なのはこの名前だけです。値は不要です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLD
KTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw
+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHEl2KhDEvv+yQzxwfEz2cl7Ef5iMr8LgGcDK7
qvMcvrgUqx68JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGwpS253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V
7flBqecH7+kVrU01F6oFzr0zM1kMyLr5HhlVDh7B0k9wp0dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtP
K6t1gFJyOn0s7QdNQ7q9knsPJsekRAH9hrLBhWBLTU/3B1QS94wEGD2YTuiW36TiP14hYwOlCAYRj2/bY3+lYz
Vu7EmzMQ+UefYxh4cF2gYD8RZL2RwmP9JV5148I3XBFPNUw/3V5jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyx
jzMd88DVzM41LxxaUDhbcmkoHT9ImzBvKzJX0J+o7FoUDFOxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4M
lHGH+0CPscZXqoi/kon9YmGauHyRs+0m6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdahuq5S
xbUzjY2JxQnrUtwB977NCzYu2sOtN+dsEReWJ6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdRKa5p3N0Nfq6RM
6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8VbaR15ivkE8dSCzuf/AInHtCzuQ6wApzEp9CUoG8/dapWriH
jNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEd
MIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Path=/
```

図 8-9 に、HTTP アナライザによる認証クッキーの出力例を示します。これは一例です。出力内容は Web サイトによって大幅に異なることがあります。

図 8-9　HTTP アナライザの出力例に表示された認証クッキー



1	認証クッキー

認証の成否に関わらず同じクッキーがサーバによって設定される場合があります。このようなクッキーは SSO の目的上、認められません。

ステップ 7　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、「失敗した」クッキーと「成功した」クッキーとをステップ 1 からステップ 6 を繰り返して比較します。

これで、HTTP Form プロトコルによる SSO をセキュリティ アプライアンス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。

HTTP Form プロトコルによる SSO の設定

この項では、前の項で収集したパラメータを使用して、HTTP Form プロトコルによる SSO の設定例を示します。この手順には、必須の手順と、条件によって必要になる手順が含まれます。必須の手順は、次の内容の設定です。

- action URI
- ユーザ名パラメータ
- パスワード パラメータ

その他の手順は、認証 Web サーバが必要とする場合にだけ必要になります。これらの設定内容は、次のとおりです。

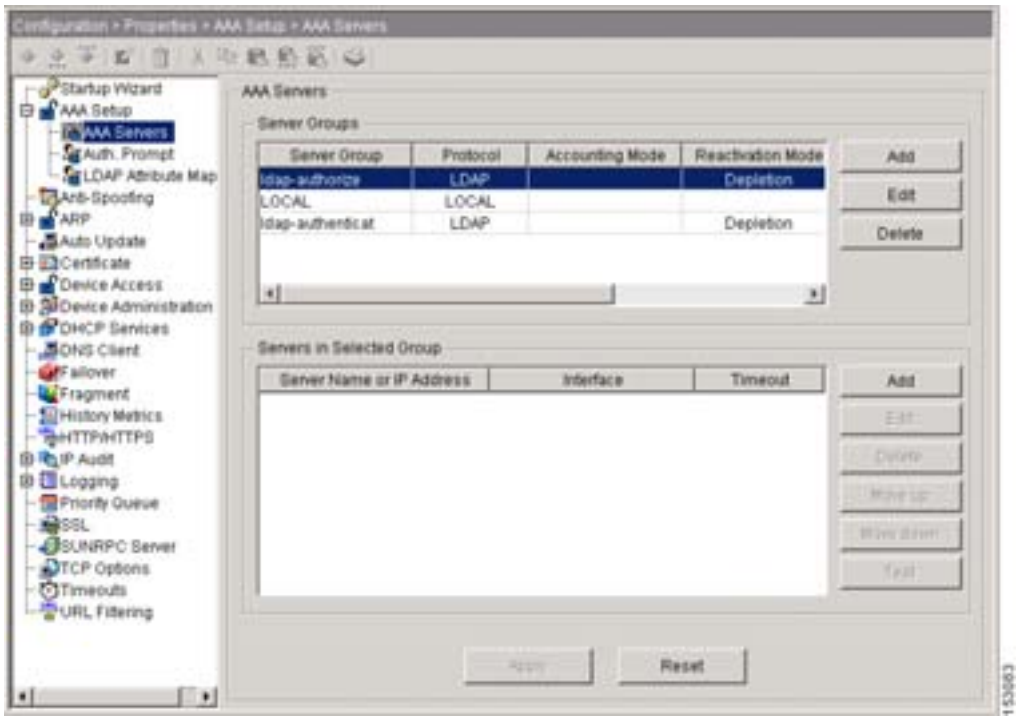
- 開始 URL
- 非表示パラメータ
- 認証クッキーの名前

次の手順を実行して、SSO で HTTP Form プロトコルを使用するようにセキュリティ アプライアンスを設定します。

ステップ 1　Cisco ASDM メイン ウィンドウで、**Configuration** > **Properties** > **AAA Setup** > **AAA Servers** を選択します。

図 8-10 のように、ウィンドウに AAA Servers 領域が表示されます。

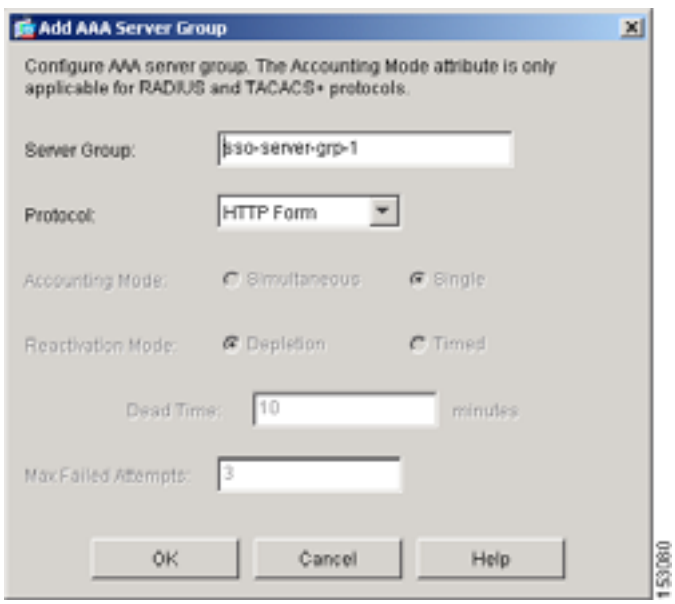
図 8-10　AAA Servers 領域が表示された ASDM ウィンドウ



ステップ 2　Server Groups 領域で **Add** をクリックします。

図 8-11 のように、Add AAA Server Group ダイアログボックスが表示されます。

図 8-11　Add AAA Server Group ダイアログボックス



ステップ 3　Server Group フィールドにサーバ グループの名前を入力します。

この例では、サーバ グループの名前は sso-server-grp-1 です。

ステップ 4　Protocol メニューから、**HTTP Form** を選択します。

他のダイアログボックスの要素が使用できなくなります。

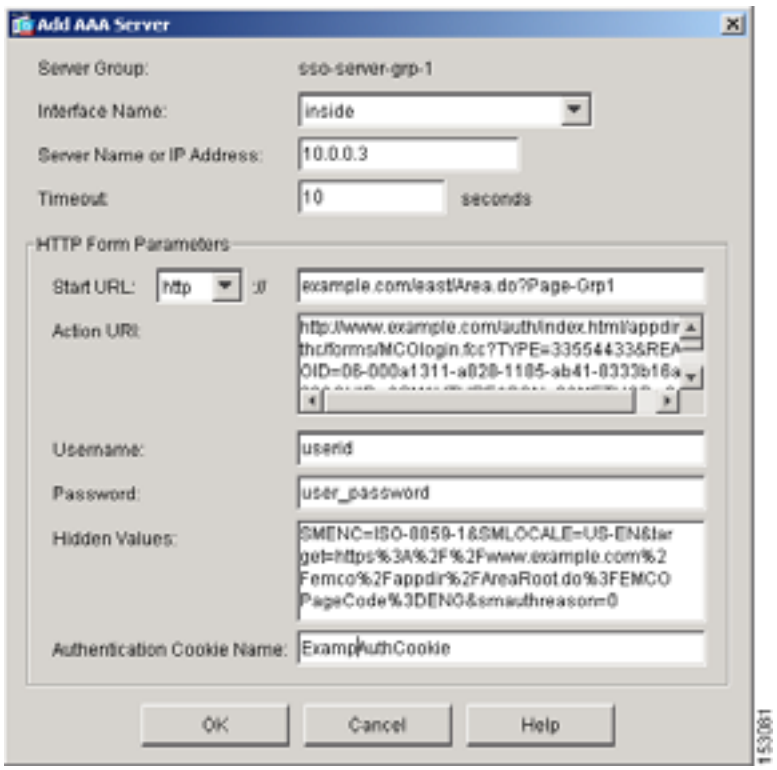
ステップ 5　**OK** をクリックして、ASDM ウィンドウに戻ります。

ステップ 6　選択されていない場合は、作成または選択したばかりのサーバ グループをクリックします。

ステップ 7　Servers in Selected Group 領域で **Add** をクリックします。

Add AAA Server ダイアログボックスが表示されます。図 8-12 は、このダイアログボックスをステップ 8 からステップ 16 に記載された値を入力した状態です。

図 8-12　Add AAA Server ダイアログボックス



ステップ 8　Interface Name メニューから、**inside**、**outside**、または **management** を選択します。

この例では、**inside** を選択します。選択したインターフェイス名は、機能に影響しません。

ステップ 9　Server Name or IP Address フィールドに、認証 Web サーバの名前またはアドレスを入力します。

この例では、内部 IP アドレスを入力します。

ステップ 10 Timeout フィールドに、失敗した SSO 認証がタイムアウトするまでの時間を秒単位で入力します。

ステップ 11 認証 Web サーバが事前ログイン クッキーを設定する場合は、次の手順を実行して、Web サーバから事前ログイン クッキーを取得するための開始 URL を設定します。

a. Start URL メニューから、次のいずれかを選択します。
- **http**（セキュリティ アプライアンスと Web サーバ間の非暗号化メッセージング用）
  または
- **https**（セキュリティ アプライアンスと Web サーバ間のセキュアなメッセージング用）

b. Start URL フィールドに、認証 Web サーバの開始 URL の後の部分を入力します。

この例では、完全な開始 URL は http://example.com/east/Area.do?Page-Grp1 です。

ステップ 12 action URI フィールドに、Web サーバの認証プログラム用の URI を入力します。

URI 全体の最大文字数は 2048 です。action URI の出力例は次のとおりです。

```
http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&R
EALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGEN
TNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%
3A%2F%2Fauth.example.com
```

（注） action URI に、ホスト名とプロトコルを含める必要があります。上記の例では、http://www.example.com の URL の最初の部分に表示されます。

ステップ 13 Username フィールドに、HTTP POST 要求のユーザ名パラメータの名前を入力します。

この例では、ユーザ名パラメータは userid という名前です。

ステップ 14 Password フィールドに、HTTP POST 要求のパスワード パラメータの名前を入力します。

この例では、パスワード パラメータは user_password という名前です。

ステップ 15 Web サーバが POST 要求で非表示パラメータを要求する場合、Hidden Values フィールドに要求された非表示パラメータを入力します。

この例では、Hidden Values エントリは次のとおりです。

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

このエントリ（POST 要求から抜粋）には、間を & で区切った 4 つのフォーム エントリとその値が含まれています。4 つのエントリとその値は次のとおりです。

- SMENC および ISO-8859-1 の値
- SMLOCALE および US-EN の値
- target および https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG の値
- smauthreason および 0 の値

ステップ 16 Authentication Cookie Name フィールドに、認証クッキーの名前を入力します。このステップはオプションです。

この例では、認証クッキー名は ExampAuthCookie です。

ステップ 17 **OK** をクリックして、ASDM ウィンドウに戻ります。

ステップ 18 **Apply** をクリックして、新しい SSO サーバとサーバ グループを実行コンフィギュレーションに追加します。

トンネル グループへの SSO サーバの割り当て

最後のタスクでは、新しい SSO サーバを新しいトンネル グループまたは既存のトンネル グループに割り当てます。この例では、次の手順を実行して、WebVPNGroup1 という名前の新しい WebVPN トンネル グループに SSO サーバを割り当てます。

ステップ 1 Cisco ASDM メイン ウィンドウで、**Configuration > VPN > General > Tunnel Group** を選択します。

ステップ 2 **Add** をクリックし、**WebVPN Access** を選択します。

General タブと Basic タブを表示した状態の Add Tunnel Group ダイアログボックスが表示されます。

ステップ 3 Name フィールドに新しいトンネル グループの名前を入力します。

この例では、名前は WebVPNGroup1 です。

ステップ 4 **AAA** タブをクリックし、Authentication Server Group メニューから新しい SSO サーバ グループを選択します。

この例では、サーバ グループの名前は sso-server-grp-1 です。

ステップ 5 **OK** をクリックして、**Configuration > VPN > General > Tunnel Group** ウィンドウに戻ってから、**Apply** をクリックし、トンネル グループを実行コンフィギュレーションに追加します。

CHAPTER 9

ネットワーク アドミッション コントロールの設定

この章には、次の項があります。

用途、要件、および制約

ネットワーク アドミッション コントロール（NAC）は、実稼働状態でのネットワーク アクセスの条件として、エンドポイントにおける準拠性チェックと脆弱性チェックを実行することによって、ワーム、ウイルス、危険なアプリケーションの侵入や感染から企業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。ポスチャ検証を設定すると、IPSec セッションを確立するアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入防止ソフトウェアが最新の状態であることを確認できます。ポスチャ検証では、リモート ホストで実行されているアプリケーションが、最新の修正プログラムによって更新されていることも確認できます。NAC は、IPSec や他のアクセス方式が提供するアイデンティティ ベースの検証を補完します。これは、ホーム PC など、ネットワーク ポリシーの自動適用の対象になっていないホストから企業ネットワークを保護する場合に特に便利です。

（注） NAC をサポートするように設定されている場合、セキュリティ アプライアンスが Cisco Secure Access Control Server のクライアントとして機能するため、ネットワーク上に少なくとも 1 台の Cisco Secure Access Control Server をインストールして NAC 認証サービスを提供する必要があります。ASA による NAC のサポートは、リモート アクセス IPSec と L2TP over IPSec セッションに限られます。ASA 上の NAC は、WebVPN、VPN 以外のトラフィック、IPv6、およびマルチモードをサポートしません。

Access Control Server への接続の設定

次の各項の説明では、少なくとも 1 台の Access Control Server をネットワークに追加して NAC をサポートしていると想定します。

- Access Control Server グループの設定（P.9-2）
- ACS グループへの ACS の追加（P.9-4）
- ACS Server Group を NAC Authentication Server として割り当てる（P.9-6）

Access Control Server グループの設定

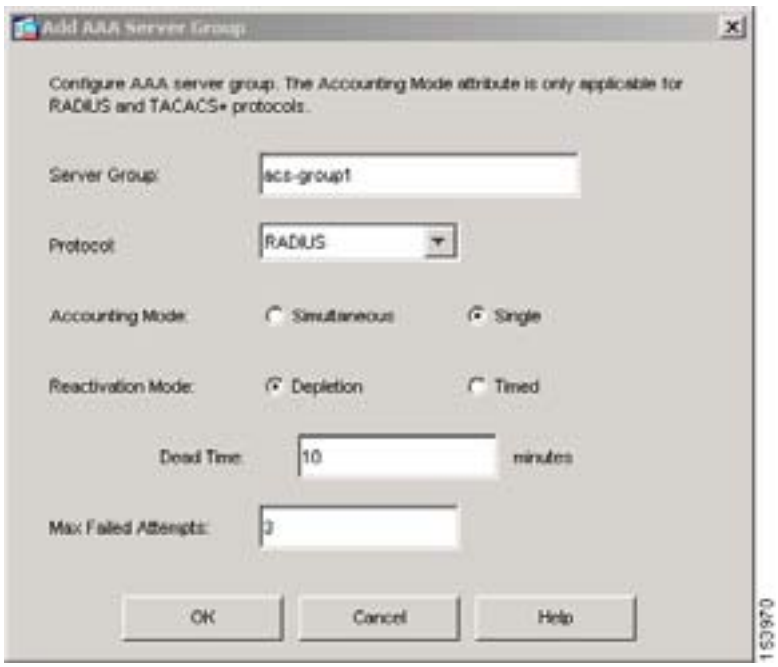
Access Control Server がネットワーク上に 1 台しかない場合でも、Access Control Server グループを設定する必要があります。

Access Control Server グループを設定する手順は、次のとおりです。

ステップ 1　Configuration > Properties > AAA Setup > AAA Server Groups を選択し、AAA Server Groups テーブルの右側の **Add** をクリックします。

AAA Server Groups ウィンドウが開きます（図 9-1）。

図 9-1　Add AAA Server Group ウィンドウ



ステップ 2　次の説明に従って、このウィンドウのアトリビュートに値を割り当てます。

- **Server Group**：サーバ グループの名前を入力します。

（注） RADIUS サーバが Class アトリビュート（#25）を返すように設定されている場合、セキュリティ アプライアンス は、そのアトリビュートを使用してグループ名を認証します。RADIUS サーバ上で、アトリビュートは OU=*groupname* という形式を取ります。ここで *groupname* は、セキュリティ アプライアンス 上の Server Group で指定したサーバ グループ名です。

- **Protocol**：これが RADIUS か LDAP サーバ グループかを指定します。Access Control Server グループの **RADIUS** を選択します。
- **Accounting Mode**：（RADIUS および TACACS+ プロトコルのみ）**Simultaneous** をクリックすると、セキュリティ アプライアンス が課金データをグループ内のすべてのサーバに送信するように設定され、**Single** をクリックすると、課金データが 1 つのサーバだけに送信されます。
- **Reactivation Mode**：**Depletion** をクリックすると、サーバに障害が起こった場合、グループ内のすべてのサーバが非アクティブになった後でサーバが再度アクティブ化して接続されます。**Timed** をクリックすると、ダウンタイムが 30 秒経過した後、障害が起こったサーバが再度アクティブ化されます。
- **Dead Time**：（Depletion モードの場合のみ）グループ内の最後のサーバが無効になってから、すべてのサーバを再度有効にするまでの分数を入力します。
- **Max Failed Attempts**：1 ～ 5 の範囲の整数を入力して、セキュリティ アプライアンス が何度接続を試みて失敗した後に、サーバの無応答、非アクティブを宣言するかを設定します。

ステップ 3　**OK** をクリックします。

AAA Server Groups テーブルに追加したグループが、Configuration > Properties >AAA Setup > AAA Server Groups テーブルに表示されます。

サーバをグループに追加するには、次の項の手順を実行します。

ACS グループへの ACS の追加

1 つ以上の Access Control Servers を ACS グループに追加する手順は、次のとおりです。

ステップ 1　Configuration > Properties > AAA Setup > AAA Server Groups を選択します。

AAA Server Groups テーブルに、このセキュリティ アプライアンスに設定されたグループが表示されます。

ステップ 2　前の項で作成した ACS グループを選択します。

グループが強調表示され、選択したグループ テーブルの Servers に、そのグループに含まれるサーバが表示されます。

ステップ 3　選択したグループ テーブルで、Servers の右側の **Add** をクリックします。

Add AAA Server ウィンドウが開きます（図 9-2）。

図 9-2　Add AAA Server ウィンドウ

ステップ 4　ACS に設定した値と同じ値を、このウィンドウのアトリビュートに値を割り当てます。アトリビュートの説明を以下に示します。

- **Server Group**：表示のみ。ACS サーバを追加するサーバ グループの名前が表示されます。
- **Interface Name**：セキュリティ アプライアンスがサーバへの接続に使用するネットワーク インターフェイスを選択します。
- **Server Name or IP Address**：AAA サーバの名前と IP アドレスを入力します。
- **Timeout**：タイムアウト間隔を秒数で入力します。セキュリティ アプライアンスは、この時間が期限切れになると、AAA サーバへの要求を放棄します。設定の中にスタンバイ AAA サーバが存在する場合に、プライマリ サーバへの接続がタイムアウトすると、セキュリティ アプライアンス が要求をバックアップ サーバに送信します。
- **Server Authentication Port**：ユーザ認証に使用するサーバのポート番号を入力します。デフォルト ポートは 1645 です。

（注）　最新の RFC では、RADIUS を UDP ポート番号 1812 に設定すべきだとしているので、このデフォルトは 1812 への変更が必要になる場合があります。

- **Server Accounting Port**：ユーザ課金に使用するサーバ ポートを入力します。デフォルト ポートは 1646 です。
- **Retry Interval**：サーバにクエリを送信し、応答がない場合に、再接続を試みるまでの秒数を入力します。秒数は、1 ～ 10 の範囲で入力します。デフォルト値は 10 秒です。
- **Server Secret Key**：暗号化に使用する、たとえば C8z077f のようなサーバ秘密鍵（「共有秘密鍵」とも呼ばれます）を入力します。この秘密鍵では、大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。セキュリティ アプライアンスは、Access Control Server への認証に、サーバ秘密鍵を使用します。ここで設定したサーバ秘密鍵は、Access Control Server で設定されたサーバ秘密鍵と一致する必要があります。最大フィールド長は、64 文字です。
- **Common Password**：グループの共通パスワードを入力します。パスワードは、大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。RADIUS サーバを許可ではなく認証に使用するよう定義する場合は、共通パスワードを設定しないでください。

  RADIUS 認証サーバでは、接続しようとする各ユーザのパスワードとユーザ名が必要です。パスワードはここに入力します。RADIUS 許可サーバの管理者は、このパスワードをセキュリティ アプライアンス経由で接続する各ユーザに関連付けて RADIUS サーバを設定する必要があります。この情報は、必ず RADIUS サーバの管理者に提供してください。このセキュリティ アプライアンス経由で RADIUS 許可サーバにアクセスするすべてのユーザの共通パスワードを入力します。

  このフィールドを空白のままにすると、各ユーザのユーザ名がパスワードになります。セキュリティ上の予防措置として、RADIUS 許可サーバを絶対に認証に使用しないでください。共通パスワードを使用したり、ユーザ名をパスワードとして使用したりすることは、各ユーザが強力なパスワードを持つことに比べて安全性が大きく劣ります。

（注）　RADIUS プロトコルではパスワード フィールドが必須であり、RADIUS サーバによっても要求されますが、ユーザはパスワードを知る必要がありません。

- **ACL Netmask Convert**：セキュリティ アプライアンスが、ダウンロード可能なアクセス リストで受け取ったネットマスクを処理する方法を選択します。セキュリティ アプライアンスは、ダウンロード可能なアクセス リストに、標準のネットマスク表現が含まれていると想定します。

ワイルドカード マスクには、無視するビット位置に 1 が、一致するビット位置に 0 が入っています。ACL Netmask Convert リストは、ダウンロード可能なアクセス リストの RADIUS サーバ上での設定方法の違いによる影響を最小限に抑えます。

Detect Automatically を選択すると、使用されているネットマスク表現のタイプをセキュリティ アプライアンスが判定します。ワイルドカード ネットマスク表現が検出された場合は、標準のネットマスク表現に変換されます。しかし、一部のワイルドカードは明確な検出が困難であるため、この設定を使用すると、ワイルドカード ネットマスク表現が、標準のネットマスク表現と誤解される場合があります。

Standard を選択すると、セキュリティ アプライアンスは、RADIUS サーバから受け取ったダウンロード可能なアクセス リストに、標準ネットマスク表現だけが入っていると想定します。セキュリティ アプライアンスは、ワイルドカード ネットマスク表現を変換しません。

Wildcard を選択すると、セキュリティ アプライアンスは、RADIUS サーバから受け取ったダウンロード可能なアクセス リストに、ワイルドカード ネットマスク表現だけが含まれていると想定し、アクセス リストがダウンロードされたときにすべてを標準ネットマスク表現に変換します。

ステップ 5　**OK** をクリックします。

選択したグループ テーブルの Servers に、追加したサーバが表示されます。

ACS サーバをサーバ グループに追加したら、次の項の手順に従って、サーバ グループをグループ ポリシーに割り当てます。

ACS Server Group を NAC Authentication Server として割り当てる

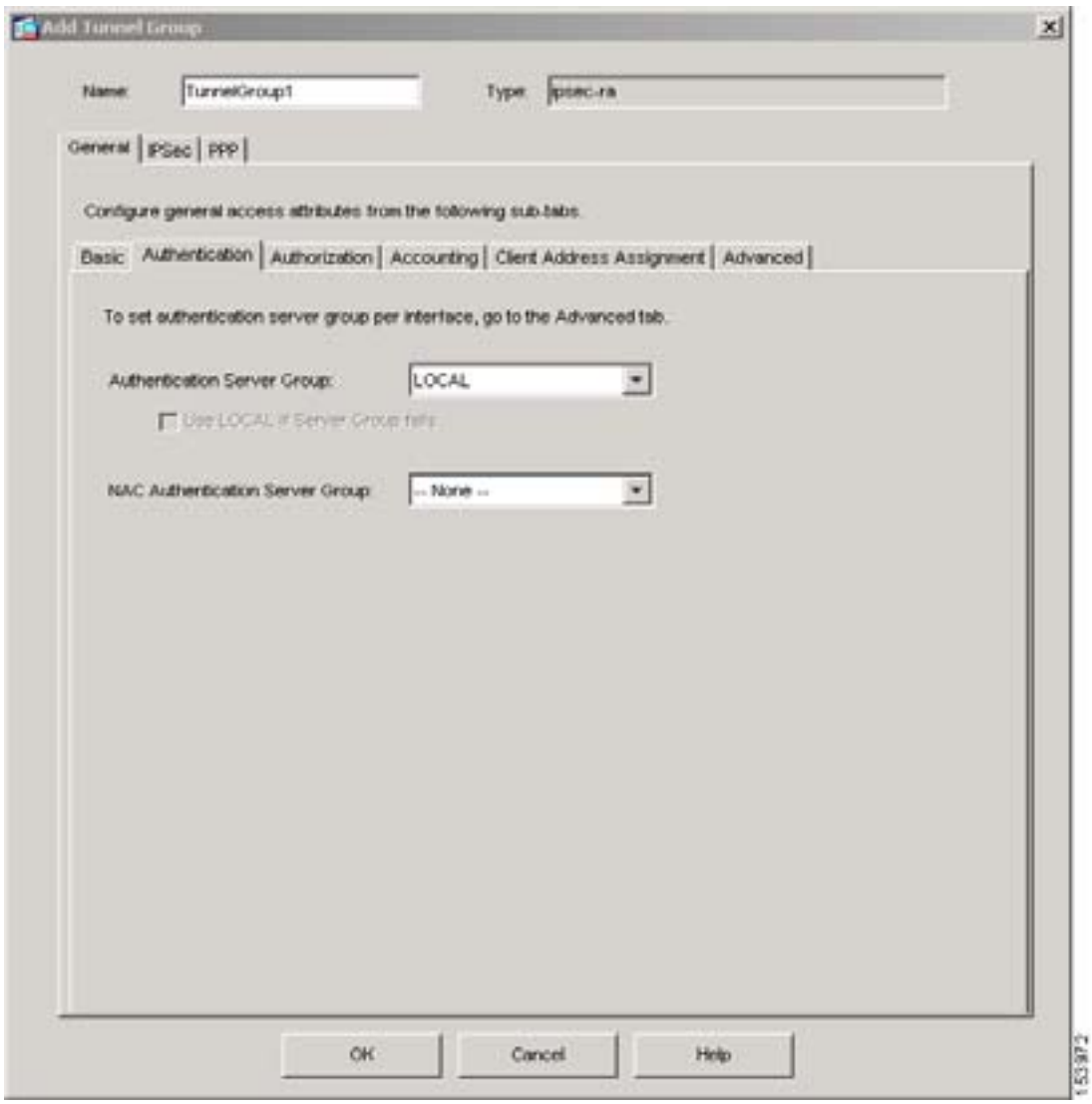
ACS Server Group を デフォルト トンネル グループの NAC Authentication Server として追加するか、または NAC のサポートを設定する代替トンネル グループに追加します。手順は次のとおりです。

ステップ 1　Configuration > VPN > General > Tunnel Group を選択します。

ステップ 2　DefaultRAGroup というトンネル グループをダブルクリックするか、リモート アクセス用に設定され、NAC サポートを設定する代替のトンネル グループ（Type は「ipsec-ra」）をダブルクリックするか、**Add** > **IPSec for Remote Access** をクリックして新しいトンネル グループを追加します。

ステップ 3　General タブ > Authentication タブをクリックします（図 9-3）。

図 9-3　General タブ > Authentication タブ



ステップ 4　次の手順に従って、このウィンドウのアトリビュートを設定します。

- **Authentication Server Group**：LOCAL グループ（デフォルト設定）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 以外のオプションを選択すると、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（Advanced タブでは、各インターフェイスに認証サーバ グループを割り当てられます）。
- **Use LOCAL if Server Group fails**：このアトリビュートをオンにすると、Authentication Server Group アトリビュートによって指定されたグループに障害が発生した場合、LOCAL データベースにフォールバックできます。フォールバックを無効にするには、このアトリビュートをオフにします。
- **NAC Authentication Server Group**：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。このセキュリティ アプライアンスに設定され、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 グループ名が一覧表示されます。

ステップ 5　**OK** をクリックします。

NAC の有効化と NAC プロパティのグループ ポリシーへの割り当て

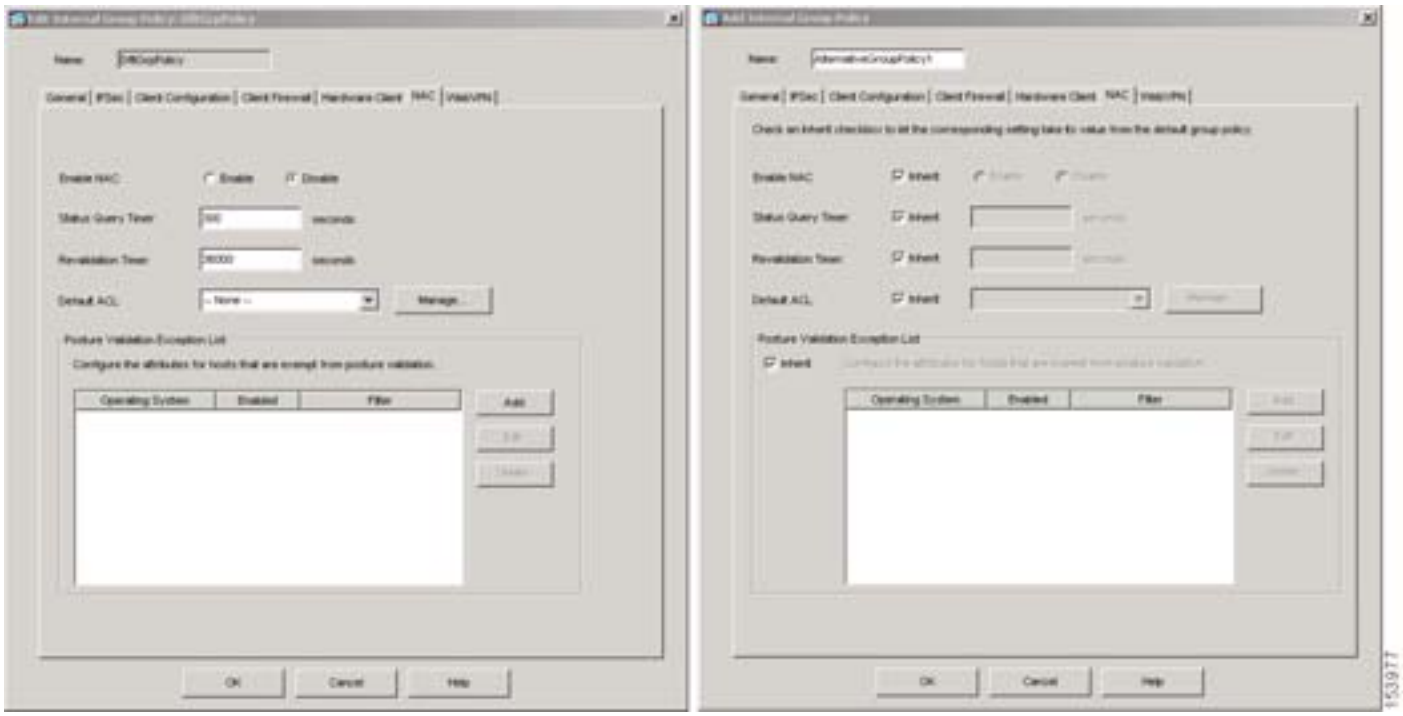
デフォルトのグループ ポリシー、または代替 IPSec グループ ポリシーで NAC を有効化し、そのデフォルト設定を表示して変更する手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Group Policy を選択します。

ステップ 2　DfltGrpPolicy というポリシーをダブルクリックするか、リモート アクセス用に設定され、NAC サポートを有効にする代替のグループ ポリシー（Tunneling Protocol は「IPSec」）をダブルクリックするか、**Add** > **Internal Group Policy** をクリックして新しいグループ ポリシーを追加します。

ステップ 3　NAC タブを開きます（図 9-4）。

図 9-4　DfltGrpPolicy の NAC タブと Alternative Group Policy



（注） Alternative Group Policy の Inherit チェックボックスをオンにすると、デフォルトのグループ ポリシーの設定がポリシーとして使用されます。Inherit チェックボックスをオフにすると、デフォルト グループ ポリシー設定とは別個に代替グループ ポリシー設定をカスタマイズできます。

ステップ 4　次の手順に従って、このウィンドウのアトリビュートを設定します。

- **Enable NAC**：**Enable** をオンにすると、Network Admission Control プロシージャが実行されて、このグループ ポリシーに関連付けられた適格なホストが検証され、ポスチャ検証チェックに合格した場合は、それらに対して Access Control Server からダウンロードされた ACL が割り当てられます。**Disable** をオンにすると、NAC プロシージャは実行されません。

(注)　その他のアトリビュートは、NAC が有効な場合にだけ有効です。

- **Status Query Timer**：ポスチャ検証に合格するたびにセキュリティ アプライアンスがステータス クエリ タイマーを起動します。このタイマーが期限切れになると、リモート ホストに対してクエリが起動され、最後のポスチャ検証以降の変更点が問い合せられます。変更なしの応答が返された場合は、ステータス クエリ タイマーがリセットされます。ポスチャの変更を示す応答が返された場合は、無条件でポスチャの再検証が起動されます。セキュリティ アプライアンスは、再検証の間、現在のアクセス ポリシーを維持します。

  デフォルトで、ポスチャ検証合格からステータス クエリまでの間隔、およびそれ以降のステータス クエリの間隔は 300 秒（5 分）です。ステータス クエリ タイマーの値は、変更しない限り、デフォルトのグループ ポリシーからグループ ポリシーに継承されます。この値を変更するには、300 ～ 1800 秒（5 ～ 30 分）の範囲で数値を入力します。

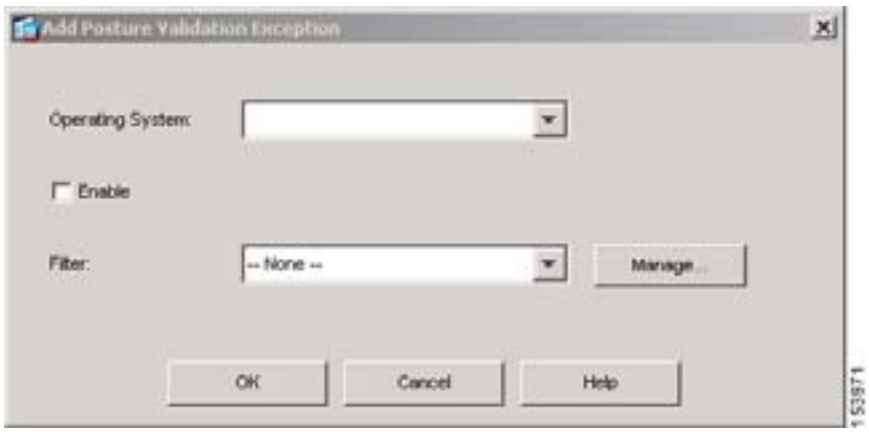
- **Revalidation Timer**：ポスチャ検証に合格するたびにセキュリティ アプライアンス が再検証タイマーを起動します。このタイマーが期限切れになると、次回のポスチャ検証が無条件で起動します。セキュリティ アプライアンスは、再検証の間、現在のアクセス ポリシーを維持します。デフォルトで、ポスチャ検証に合格してから次のポスチャ検証までの間隔は、36000 秒（10 時間）です。再検証タイマーの値は、変更しない限り、デフォルトのグループ ポリシーからグループ ポリシーに継承されます。この値を変更するには、300 ～ 86400 秒（5 分 ～ 24 時間）の範囲で数値を入力します。

- **Default ACL**：セキュリティ アプライアンスは、ポスチャ検証の前に、このアトリビュートによって識別された ACL を、NAC に適格なホストに適用します。ポスチャ検証の後、セキュリティ アプライアンスは、デフォルトの ACL の代わりに、Access Control Server からリモート ホスト用に取得した ACL を使用します。再検証に失敗した場合は、この ACL が適用されます。クライアントレス認証が有効な場合、セキュリティ アプライアンスは、Cisco Trust Agent を持たないホストにもこの ACL を適用してポスチャ検証要求に対応します。ACL を選択して NAC セッションのデフォルトの ACL として使用するか、デフォルト設定の **None** を使用してデフォルト ACL を適用しないようにします。

  ACL をドロップダウン リストに追加するには、リストに ACL の設定を表示するか、リストで ACL を変更して、**Manage** をクリックします。ACL Manager ウィンドウが開きます。手順については、P.2-14 の「ACL と ACE の管理」を参照してください。

- **Posture Validation Exception List**：Enabled カラムの Yes の値は、関連付けられたオペレーティング システムがポスチャ検証を免除されていることを示します。No の値は、設定内に免除エントリはあっても、セキュリティ アプライアンスがそれを無視していることを示します。Filter はオプションです。ポスチャ検証からのコンピュータの除外に加えて、コンピュータのオペレーティング システムが一致し、Enabled の値が Yes の場合、セキュリティ アプライアンスは Filter カラムで識別された ACL を適用して、トラフィックをフィルタリングします。リストでエントリを追加または変更するには、**Add** をクリックするか、変更するエントリをダブルクリックします。Add or Edit Posture Validation ウィンドウが開きます（図 9-5）。

図 9-5　Add Posture Validation Exception



ステップ 5　（Posture Validation Exception List を変更している場合のみ）次の手順に従って、このウィンドウのアトリビュートを設定します。

- **Operating System**：ポスチャ検証から除外するリモート コンピュータで実行されているオペレーティングシステムを選択するか、その名前を入力します。たとえば、**Windows XP** のように入力します。
- **Enable**：オンにすると免除が有効になります。デフォルト設定はオフで、免除リストから削除はされませんが、免除リストのエントリが無効になります。
- **Filter** は、コンピュータ上で動作しているオペレーティング システムが Operating System アトリビュート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。フィルタを適用しない場合は、デフォルト オプションの **None** を使用します。使用する場合は、ドロップダウン リストから ACL を選択します。

  ACL をドロップダウン リストに追加するには、リストに ACL の設定を表示するか、リストで ACL を変更して、**Manage** をクリックします。ACL Manager ウィンドウが開きます。手順については、P.2-14 の「ACL と ACE の管理」を参照してください。

  Add or Edit Posture Validation でアトリビュートを設定した後、**OK** をクリックします。NAC タブでは、Posture Validation Exception List に、新しいエントリと変更されたエントリが表示されます。

ステップ 6　**OK**、**Apply** の順にクリックして、変更内容を実行コンフィギュレーションに保存します。

グローバル NAC 設定の変更

セキュリティ アプライアンスには、すべての NAC セッションに適用するデフォルトの設定が用意されています。この項の説明に従って、ネットワークで実行されているポリシーに合わせて、これらの設定を調整します。

ASA は、セキュリティ アプライアンスとリモート ホストとの間の通信を指定するアトリビュートに対して、デフォルトの設定を提供します。これらのアトリビュートは、有効期限カウンタの最大値を決定します。この値は、リモート ホスト上の Cisco Trust Agent を制限し、Cisco Trust Agent との通信のためのポート番号を指定します。

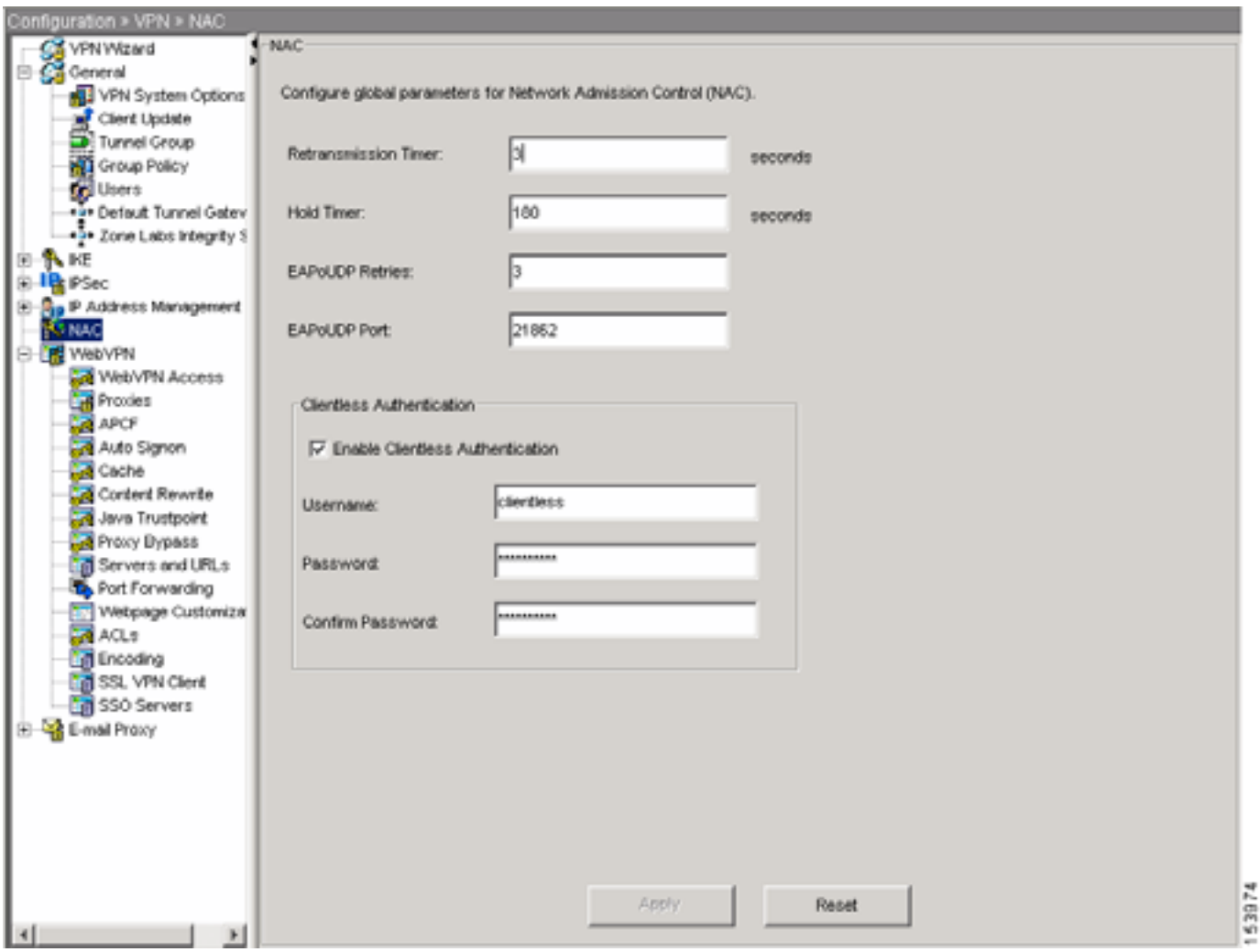
またグローバル NAC 設定では、クライアントレス認証の有効と無効を切り替えられます。この設定は、ポスチャ検証要求に応答する Cisco Trust Agent を持たないホストに対して、ポリシーを適用します。

NAC 設定を表示、変更する手順は、次のとおりです。

ステップ 1　Configuration > VPN > NAC を選択します。

ステップ 2　NAC ウィンドウが開きます（図 9-6）。

図 9-6　NAC



(注)　このウィンドウのアトリビュートは、セキュリティ アプライアンスが IPSec セッションに適用するグループ ポリシーで NAC が有効な場合にだけ有効です。

ステップ 3　次の手順に従って、このウィンドウのアトリビュートを設定します。

- **Retransmission Timer**：セキュリティ アプライアンスがリモート ホストにポスチャ検証を求める EAP over UDP 要求を送信し、応答を待ちます。このアトリビュートに割り当てられた秒数の間に応答がなければ、EAP over UDP メッセージが再送されます。デフォルトでは、再送信タイマーは 3 秒です。待ち時間の長さを変更するには、1 ～ 60 の範囲で値を入力します。
- **Hold Timer**：EAPoUDP Retries カウンタが EAPoUDP Retries の値に一致した場合、セキュリティ アプライアンスは、リモート ホストとの EAP over UDP セッションを終了して、このタイマーを再開始します。このアトリビュートが *n* 秒に等しい場合、セキュリティ アプライアンスは、リモートホストとの EAP over UDP セッションを確立します。デフォルトでは、新しいセッションを確立するまでの最大待ち時間は 180 秒です。秒数は、60 ～ 86400 （24 時間）の範囲で入力して変更します。
- **EAPoUDP Retries**：セキュリティ アプライアンスがリモート ホストに EAP over UDP メッセージを送信し、応答を待ちます。応答がなければ、EAP over UDP メッセージが再送信されます。デフォルトでは、再試行は最大 3 回行われます。この値を変更するには、1 ～ 3 の範囲で値を入力します。
- **EAPoUDP Port**：Cisco Trust Agent との EAP over UDP 通信に使用するクライアント エンドポイント上のポート番号を入力します。デフォルトのポート番号は 21862 です。この値を変更するには、1024 ～ 65535 の範囲で値を入力します。
- **Enable Clientless Authentication**：オンにすると、ポスチャ検証要求に応答する Cisco Trust Agent を持たないホストに対して、ポリシーを適用します。

  ホストが IPSec セッションの確立を試みると、セキュリティ アプライアンスはデフォルトのアクセス ポリシーを適用し、ポスチャ検証を求める EAP over UDP 要求を送信し、タイムアウトを要求します。セキュリティ アプライアンスが、クライアントレス ホストのポリシーを Access Control Server に要求するように設定されていない場合、そのクライアントレス ホストに対してすでに使用されているデフォルトのアクセス ポリシーが引き続き使用されます。

  クライアント認証が有効で、検証要求に対するリモート ホストからの応答がない場合、セキュリティ アプライアンスは、リモート ホストに代わってクライアントレス認証要求を Access Control Server に送信します。この要求には、Access Control Server 上でのクライアントレス認証用に設定されたクレデンシャルに一致するログインクレデンシャルが含まれます。Access Control Server は次にアクセス ポリシーを提供し、これがセキュリティ アプライアンスによって適用されます。

(注)　その他のアトリビュートは、**Enable Clientless Authentication** がオンの場合にだけ適用されます。

- **Username**：クライアントレス ホストをサポートするために、Access Control Server 上に設定されたユーザ名を入力します。デフォルトのユーザ名は、「clientless」です。このユーザ名を Access Control Server で変更した場合は、セキュリティ アプライアンスでも変更する必要があります。ユーザ名には、1 ～ 64 文字の ASCII 文字が入力できますが、先頭と末尾の空白、ポンド記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< と >）は使用できません。
- **Password**：クライアントレス ホストをサポートするために、Access Control Server 上に設定されたパスワードを入力します。デフォルトのパスワードは、「clientless」です。このパスワードを Access Control Server で変更した場合は、セキュリティ アプライアンスでも変更する必要があります。パスワードには、4 ～ 32 文字の ASCII 文字が使用できます。
- **Confirm Password**：Password に入力したパスワードを再度入力して確認します。

ステップ 4　**Apply** をクリックして、変更内容を実行コンフィギュレーションに保存します。

CHAPTER 10

L2TP over IPSec の設定

この章では、ASDM を使用してセキュリティ アプライアンス上に L2TP over IPSec を設定する方法について説明します。この章には、次の項があります。

L2TP の概要

Layer 2 Tunneling Protocol（L2TP）は、リモート クライアントがパブリック IP ネットワーク経由でプライベート企業ネットワーク サーバと安全に通信できる VPN トンネリング プロトコルです。L2TP は PPP over UDP（ポート 1701）を使用してデータをトンネリングします。

L2TP プロトコルは、クライアント / サーバ モデルに基づいています。この機能は、L2TP ネットワーク サーバ（LNS）と L2TP アクセス コンセントレータ（LAC）との間で分割されます。通常 LNS はルータなどのネットワーク ゲートウェイで実行され、LAC は、ダイヤルアップ ネットワーク アクセス サーバ（NAS）や、Microsoft Windows 2000 などの L2TP クライアントがバンドルされた PC などで実行されます。

IPSec を使用する L2TP をリモート アクセス シナリオで設定することの最大の利点は、リモート ユーザが、ゲートウェイや専用回線を使用せずにパブリック IP ネットワーク経由で VPN にアクセスできるため、POTS を使用してほとんどどこからでもリモート アクセスができることです。その他の利点として、クライアントの要件が、マイクロソフトの Dial-Up Networking（DUN; ダイヤルアップ ネットワーク）搭載の Windows 2000 だけであることです。Cisco VPN クライアント ソフトウェアなど、その他のクライアント ソフトウェアは必要ありません。

IPSec を使用する L2TP の設定では、事前共有鍵や RSA シグニチャ方式を使用した証明書、および動的（固定ではない）暗号マップの使用がサポートされています。このタスクの説明では、IKE と事前共有鍵または RSA シグニチャ設定が完了していると想定します。

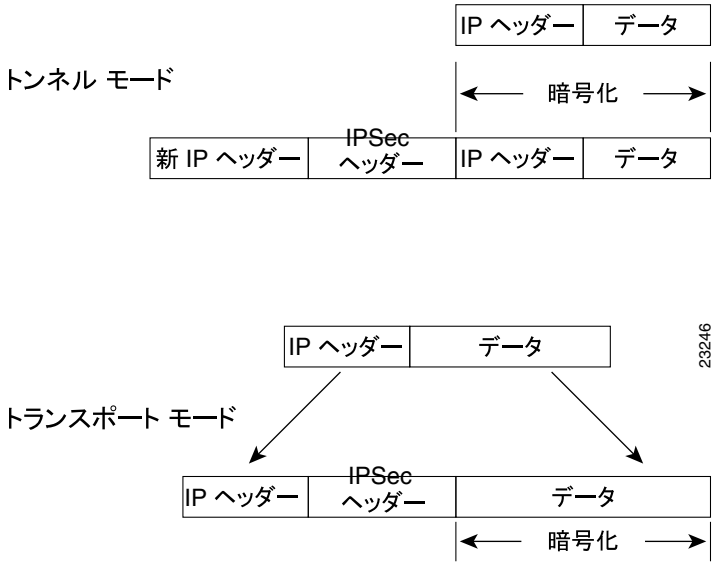
（注） セキュリティ アプライアンスで IPSec を用いる L2TP を使用すると、LNS が Windows 2000 L2TP クライアントと相互運用できます。Cisco や他のベンダーと LAC との相互運用は、現在サポートされていません。セキュリティ アプライアンスでサポートされているのは IPSec を使用する L2TP だけで、L2TP 自体はサポートされていません。
Windows 2000 クライアントによってサポートされている最小限の IPSec セキュリティ アソシエーション ライフタイムは、300 秒です。セキュリティ アプライアンスを 300 秒未満に設定すると、Windows 2000 クライアントはそれを無視して、ライフタイムを 300 秒に設定し直します。

IPSec トランスポートとトンネル モード

デフォルトで、セキュリティ アプライアンスは IPSec トンネル モードを使用します。つまり、元の IP データ グラム全体が暗号化されて、新しい IP パケット内でペイロードとなります。このモードでは、ルータなどのネットワーク デバイスが IPSec プロキシとして動作できます。言い換えると、ルータがホストの代わりに暗号化を実行するということです。発信元ルータがパケットを暗号化し、IPSec トンネル経由で転送します。宛先ルータは、元の IP データグラムを復号化し、宛先システムに転送します。トンネルモードの最大の利点は、IPSec の利点を得るためにエンド システムを変更する必要がないことです。トンネル モードはトラフィック分析を防止します。トンネル モードを使用することで、攻撃者はトンネルのエンドポイントを判別できるだけで、トンネルされたパケットの本当の発信元や宛先はわかりません。このことは、たとえ発信元や宛先がトンネル エンドポイントと同じであっても同じです。

ただし Windows 2000 L2TP/IPSec クライアントは IPSec トランスポート モードを使用しているため、IP ペイロードだけが暗号化され、元の IP ヘッダーは元のまま残されます。このモードは、各パケットにわずか数バイト追加するだけで、パブリック ネットワーク上のデバイスがパケットの最終的な発信元と宛先がわかるという利点があります。図 10-1 に、IPSec のトンネル モードとトランスポート モードの違いを示します。

図 10-1　トンネル モードとトランスポート モードの IPSec



したがって、Windows 2000 L2TP/IPSec クライアントでセキュリティ アプライアンスに接続するためには、IPSec トランスポート モードを設定してトランスフォームする必要があります（ステップ 1 を参照）。この機能（トランスポート）を使用すると、IP ヘッダー内の情報に基づいて、中間ネットワーク上で特別な処理（たとえば、QoS）を実行できます。しかし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査は制限されます。IP ヘッダーをクリア テキストで伝送した場合、トランスポート モードでは攻撃者がトラフィック分析を実行できます。

（注） セキュリティ アプライアンスに Cisco VPN Client Version バージョン 3.x またはバージョン 2.5 がインストールされていると、Windows 2000 で L2TP/IPSec トンネルを確立できません。Windows 2000 の Services パネルで、Cisco VPN Client バージョン 3.x の *Cisco VPN Service* または Cisco VPN Client バージョン 2.5 の *ANetIKE Service* を無効にします（**Start** > **Programs** > **Administrative Tools** > **Services** をクリック）。次に、**Services** パネルから IPSec Policy Agent Service を再起動し、マシンをリブートします。

L2TP over IPSec の設定

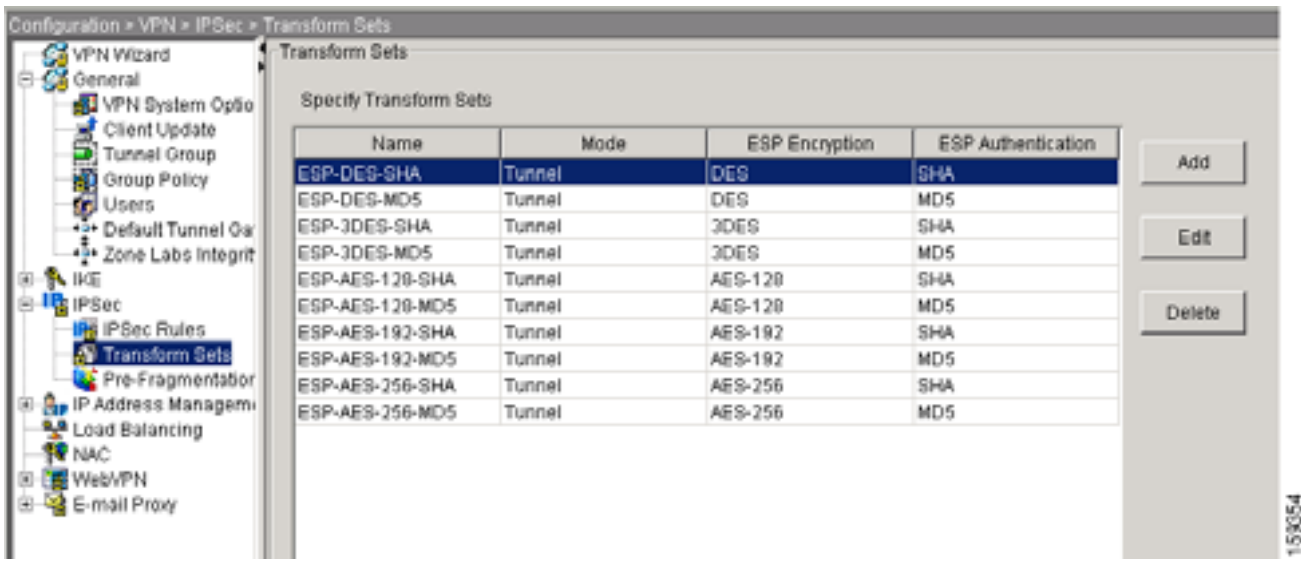
セキュリティ アプライアンスで L2TP over IPSec 接続を設定する手順は、次のとおりです。

（注） セキュリティ アプライアンスに Cisco VPN Client バージョン 3.x または Cisco VPN 3000 Client バージョン 2.5 がインストールされていると、Windows 2000 で L2TP/IPSec トンネルを確立できません。Windows 2000 の Services パネルで、Cisco VPN Client バージョン 3.x の *Cisco VPN Service* または Cisco VPN Client バージョン 2.5 の *ANetIKE Service* を無効にします（**Start** > **Programs** > **Administrative Tools** > **Services** を選択）。次に、**Services** パネルから IPSec Policy Agent Service を再起動し、マシンをリブートします。

ステップ 1　IPSec トランスフォーム セットを追加し、IPSec がトンネル モードではなく、トランスポート モードを使用するように指定します。

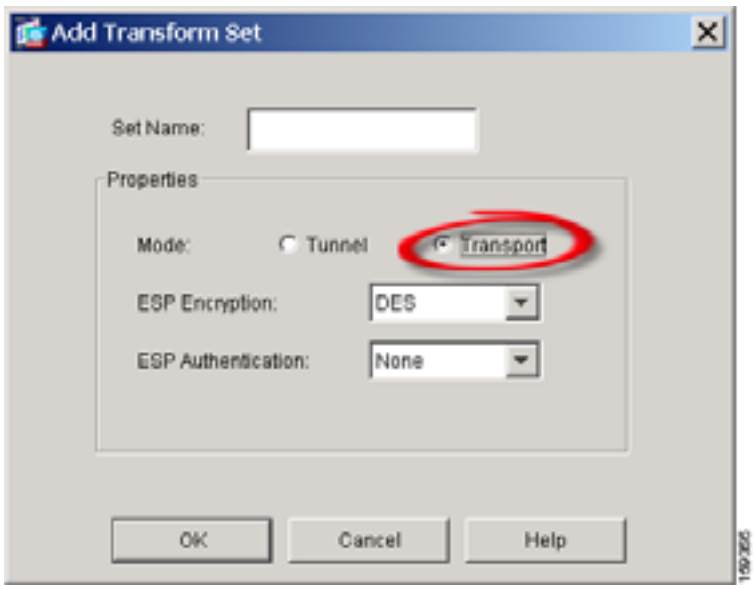
これには、**Configuration** > **VPN** > **IPSec** > **Transform Sets** を選択します。**Add** をクリックします。Transform Sets ペインが表示されます（図 10-2）。

図 10-2　Transform Sets ペイン



Add をクリックします。Add Transform Set ダイアログが表示されます（図 10-3）。

図 10-3　Add Transform Set ダイアログ

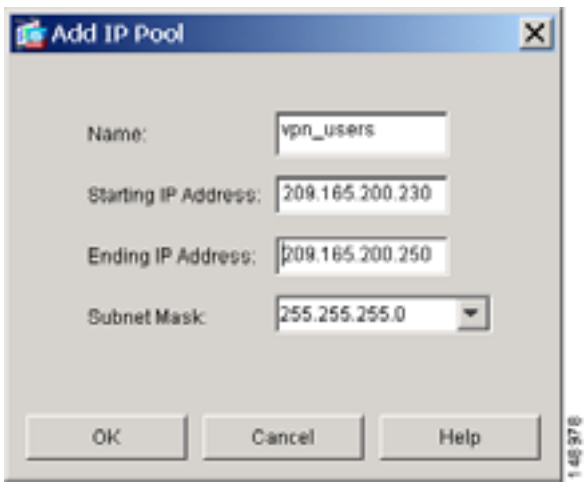


トランスフォーム セットの名前を入力します。ESP Encryption 方式と ESP Authentication 方式を選択します。**OK** をクリックします。

ステップ 2　アドレス割り当ての方式を設定します。この例では、IP アドレス プールを使用します。

IP アドレス プールを作成するには、**Configuration > VPN > IP Address Management > IP Pools** を選択します。**Add** をクリックします。Add IP Pool ダイアログが表示されます（図 10-4）。

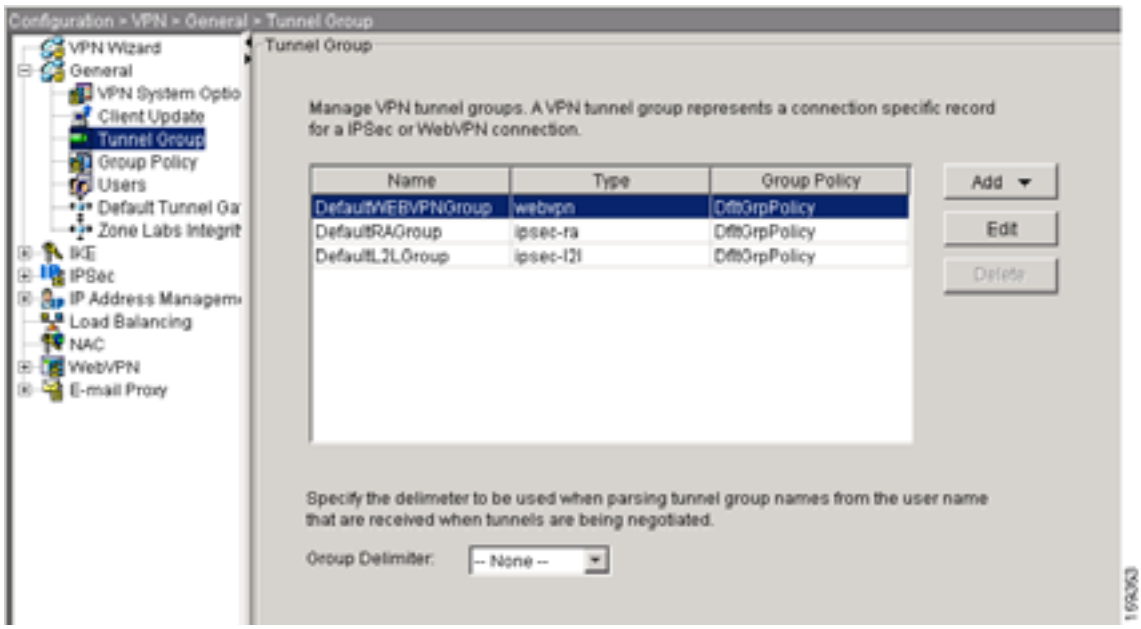
図 10-4　Add IP Pool ダイアログ



新しいアドレス プールの名前を入力します。開始 IP アドレスと終了 IP アドレスを入力し、サブネット マスクを入力して **OK** をクリックします。

ステップ 3　IP アドレス プールをトンネル グループに割り当てます。これには、**Configuration >VPN > General > Tunnel Group** を選択します。Tunnel Group ペインが表示されます（図 10-5）。

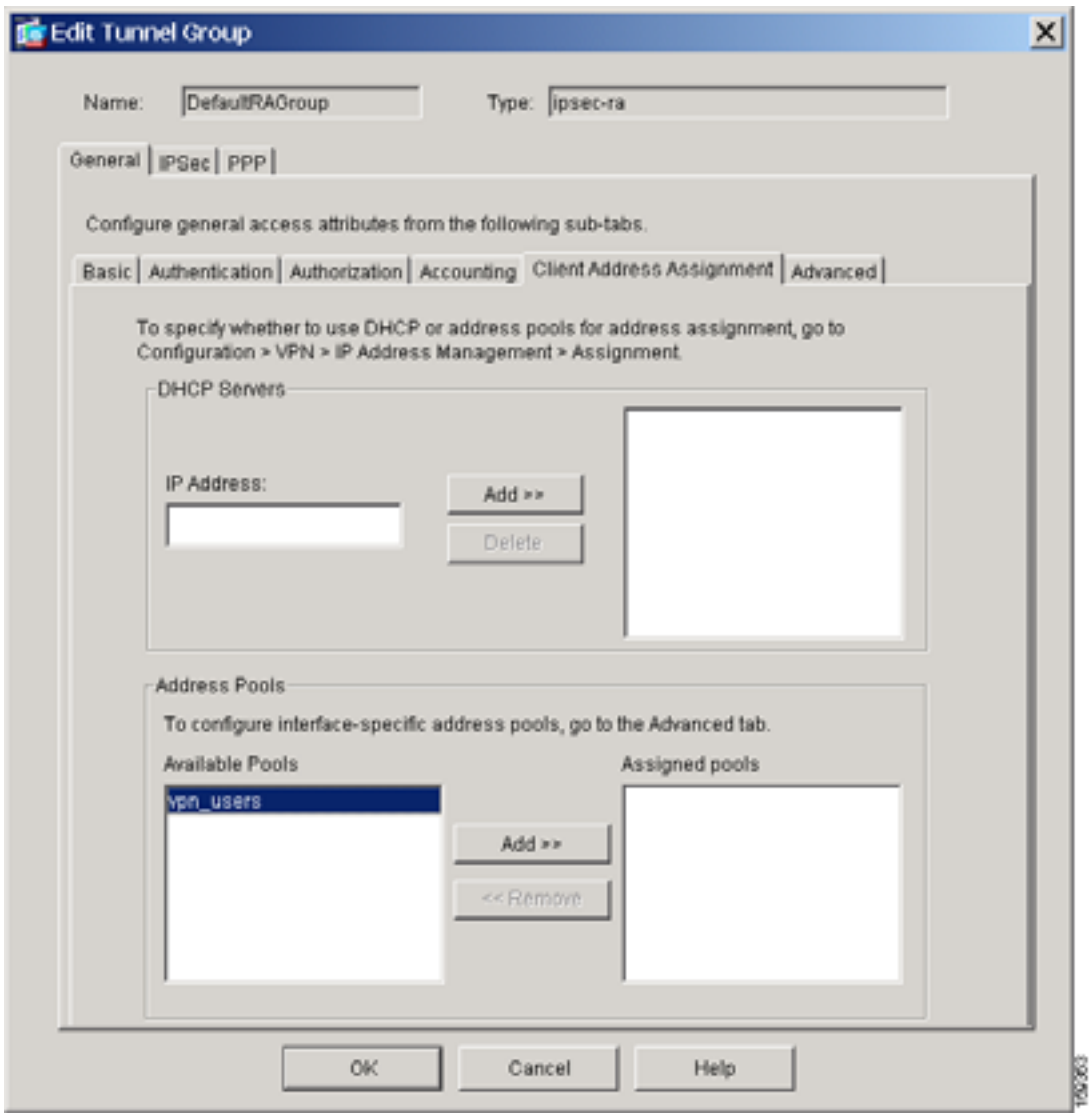
図 10-5　Tunnel Group ペイン



テーブルでトンネル グループ選択して **Edit** をクリックします。Edit Tunnel Group ダイアログが表示されます。

Client Address Assignment タブをクリックします。Client Address Assignment タブ（図 10-6）に、Address Pools グループ ボックスが表示されます。

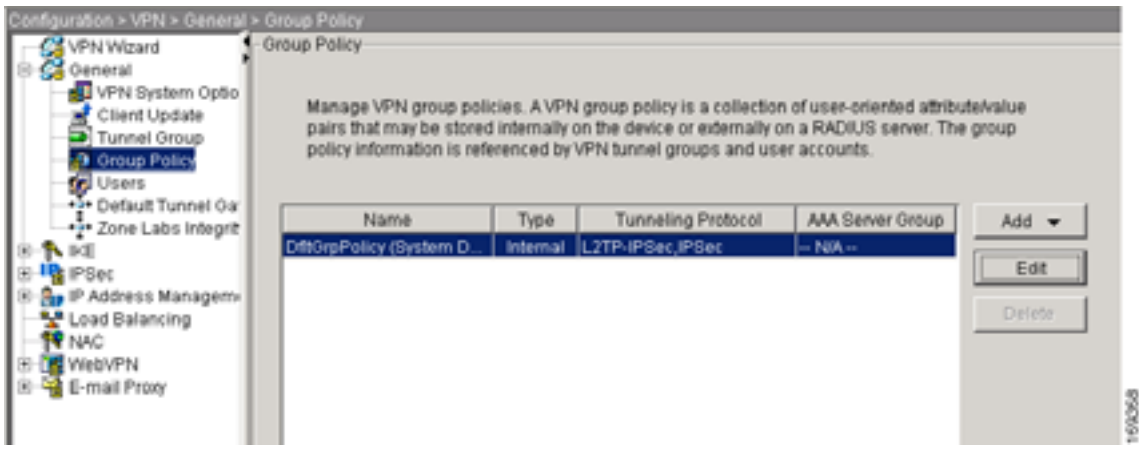
図 10-6　Edit Tunnel Group、General タブ、Client Address Assignment タブ



Address Pools 領域で、トンネル グループに割り当てるアドレス グループを選択し、**Add** をクリックします。Assigned pools ボックスに、アドレス プールが表示されます。

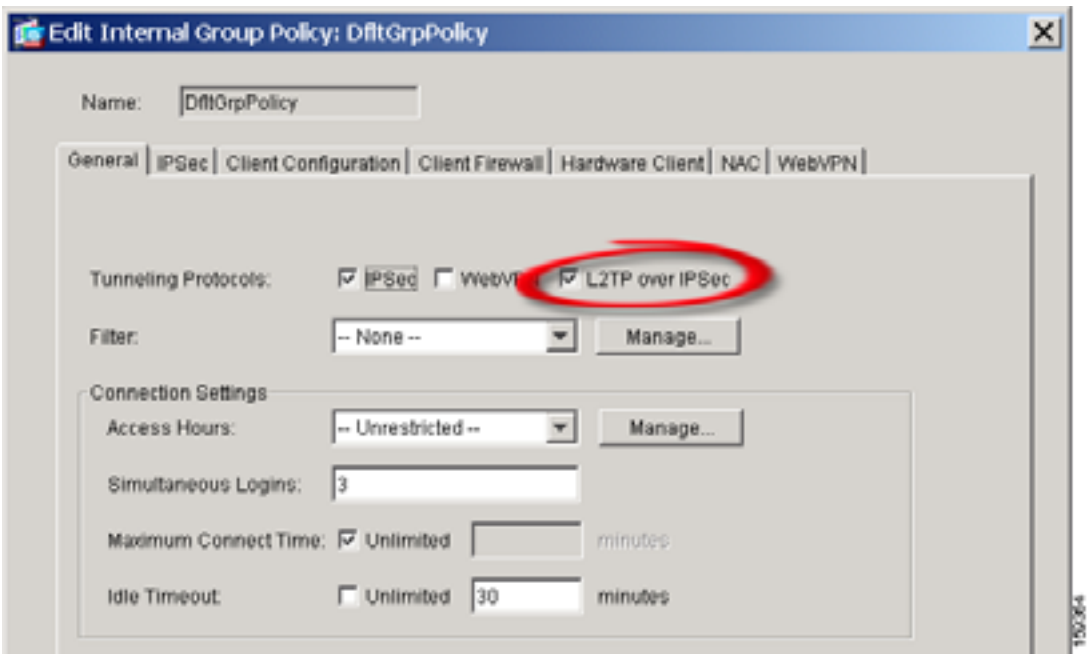
ステップ 4　L2TP over IPSec をこのグループ ポリシーの有効な VPN トンネリング プロトコルとして設定します。**Configuration > VPN > General > Group Policy** を選択します。Group Policy ペインが表示されます（図 10-7）。

図 10-7　Edit Internal Group Policy



グループ ポリシーを選択して Edit をクリックします。Edit Group Policy ダイアログが表示されます（図 10-8）。

図 10-8　Edit Group Policy ダイアログ、General タブ



L2TP over IPSec をクリックして、グループ ポリシーのプロトコルを有効にします。**OK** をクリックします。

ステップ 5　グループ ポリシーをトンネル グループにリンクし、トンネル グループ スイッチングを有効にします（オプション）。**Configuration >VPN > General > Tunnel Group** を選択して、トンネル グループの設定に戻ります。Tunnel Group ペインが表示されますトンネル グループを選択して **Edit** をクリックします。Edit Tunnel Group、General タブ、Basic タブが表示されます（図 10-9）。グループ ポリシーを選択します。

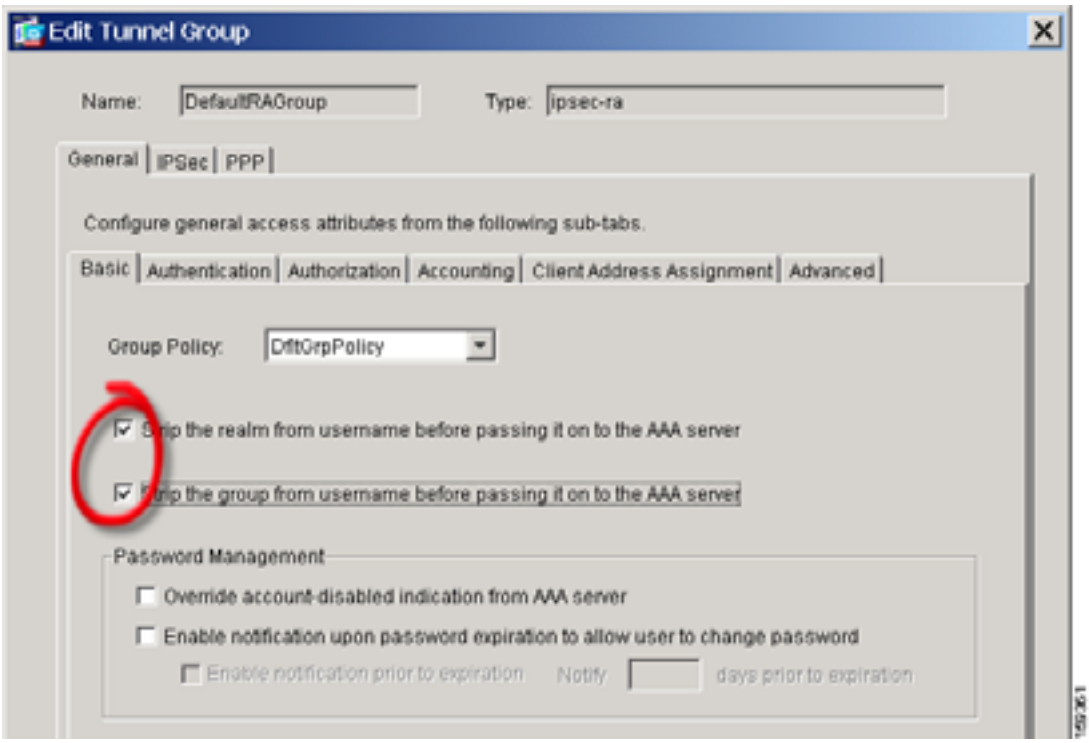
トンネル グループ スイッチングを使用すると、セキュリティ アプライアンスを、他のトンネル グループとの L2TP over IPSec 接続を確立する複数のユーザに関連付けられます。各トンネル グループには、それぞれの AAA サーバ グループと IP アドレス プールがあるため、ユーザは、各自のトンネル グループに固有の方式で認証を行えます。

この機能では、ユーザがユーザ名だけを送信するのではなく、ユーザ名とグループ名を *username@group_name* という形式で送信します。ここで、「@」は設定可能なデリミタであり、グループ名はセキュリティ アプライアンスで設定したトンネル グループ名です。

トンネル グループ スイッチングはストリップ グループ処理によって有効になります。これによりセキュリティ アプライアンスは、VPN クライアントが提供するユーザ名からグループ名を取得して、ユーザ接続のためのトンネルグループを選択できます。このようにして、セキュリティ アプライアンスは、ユーザ名のユーザの部分だけを送信して許可と認証ができます。そうでない場合（無効な場合）、セキュリティ アプライアンスはレルムも含めたユーザ名全体を送信します。

トンネル グループ スイッチを有効にするには、**Strip the realm from username before passing it on to the AAA server** をオンにし、**Strip the group from username before passing it on to the AAA server** をオンにします。**OK** をクリックします。

図 10-9　Edit Tunnel Group ダイアログ、General タブ、Basic タブ



ステップ 6　L2TP over IPSec は、PPP 認証プロトコルを使用します。トンネル グループの PPP タブで、PPP 接続に許可されるプロトコルを指定します（図 10-10）。表 10-1 は、PPP 認証のタイプとその特徴を示します。

図 10-10　Edit Tunnel Group、PPP タブ

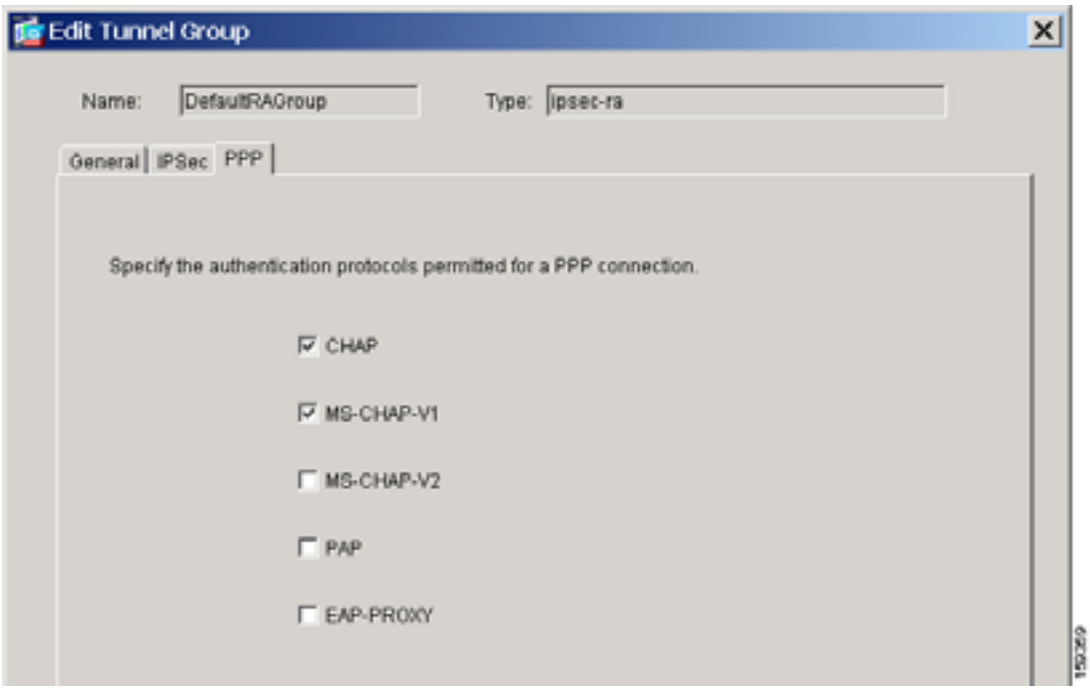


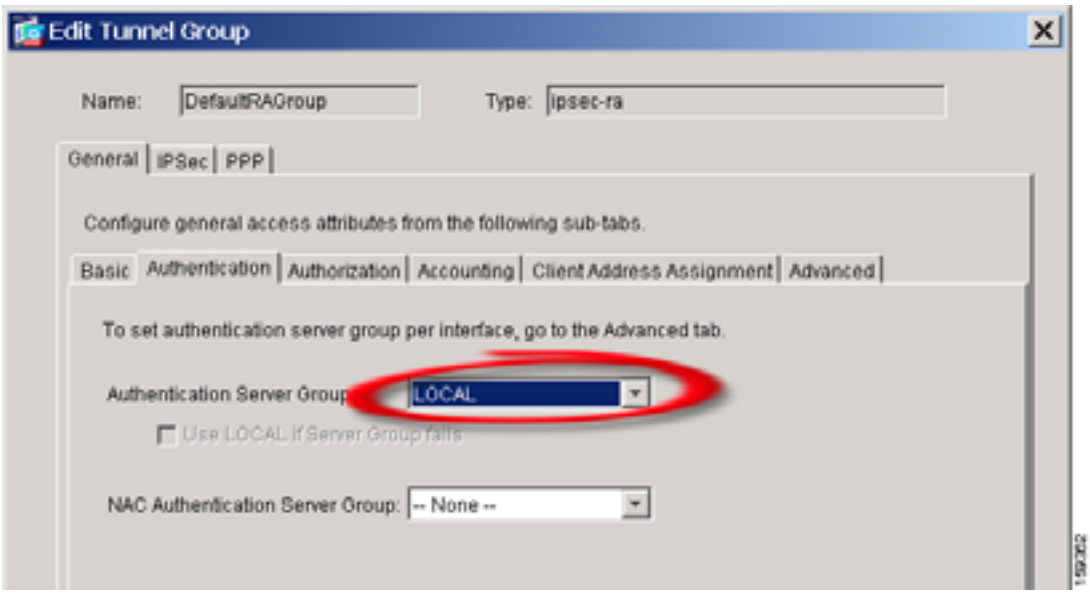
表 10-1　認証タイプの特徴

キーワード	認証タイプ	特徴
chap	CHAP	サーバのチャレンジに対して、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 よりセキュアですが、データを暗号化しません。
eap-proxy	EAP	EAP を有効にすると、セキュリティ アプライアンスが、外部の RADIUS サーバに対して PPP 認証プロセスを代行できます。
ms-chap-v1 **ms-chap-v2**	Microsoft CHAP バージョン 1 Microsoft CHAP バージョン 2	CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。このプロトコルは、MPPE によってデータの暗号化のための鍵を生成します。
pap	PAP	認証時にクリア テキストのユーザ名とパスワードを渡すため、セキュアではありません。

ステップ 7　L2TP over IPSec 接続を試みるユーザの認証方式を指定します。セキュリティ アプライアンスが認証サーバか、独自のローカル データベースかのいずれを使用するかを設定します。これには、トンネル グループの **Authentication** タブをクリックします。Authentication タブが表示されます（図 10-11）。

デフォルトで、セキュリティ アプライアンス は、ローカル データベースを使用します。つまり、Authentication Server Group ドロップダウン リストには LOCAL と表示されます。認証サーバを使用するには、リストから認証サーバを選択します。

図 10-11　Edit Tunnel Group、General タブ、Authentication タブ

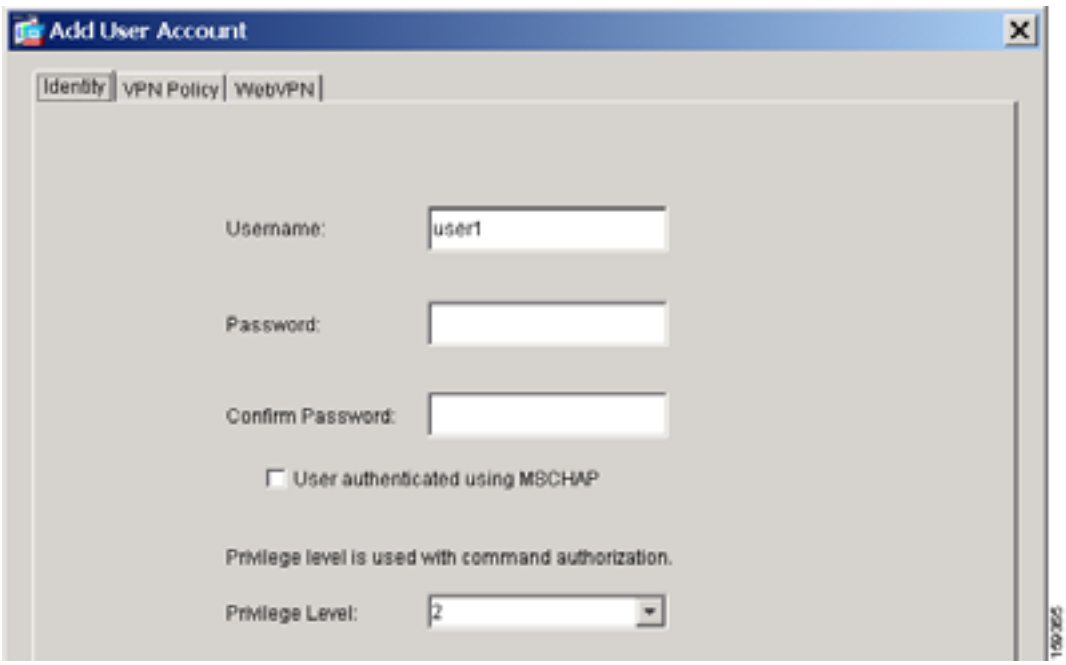


（注）　セキュリティ アプライアンスは、ローカル データベースで、PPP 認証、PAP および Microsoft CHAP バージョン 1 および 2 だけをサポートします。EAP と CHAP は、プロキシ認証サーバによって実行されます。そのため、リモート ユーザが EAP または CHAP を設定したトンネル グループに属していて、セキュリティ アプライアンスがローカル データベースを使用するように設定されている場合、ユーザは接続できません。

ステップ 8　ローカル データベースでユーザを作成します。**Configuration >Properties > Device Administration > User Accounts** を選択します。**Add** をクリックします。Add User Accounts ダイアログが開きます（図 10-12）。

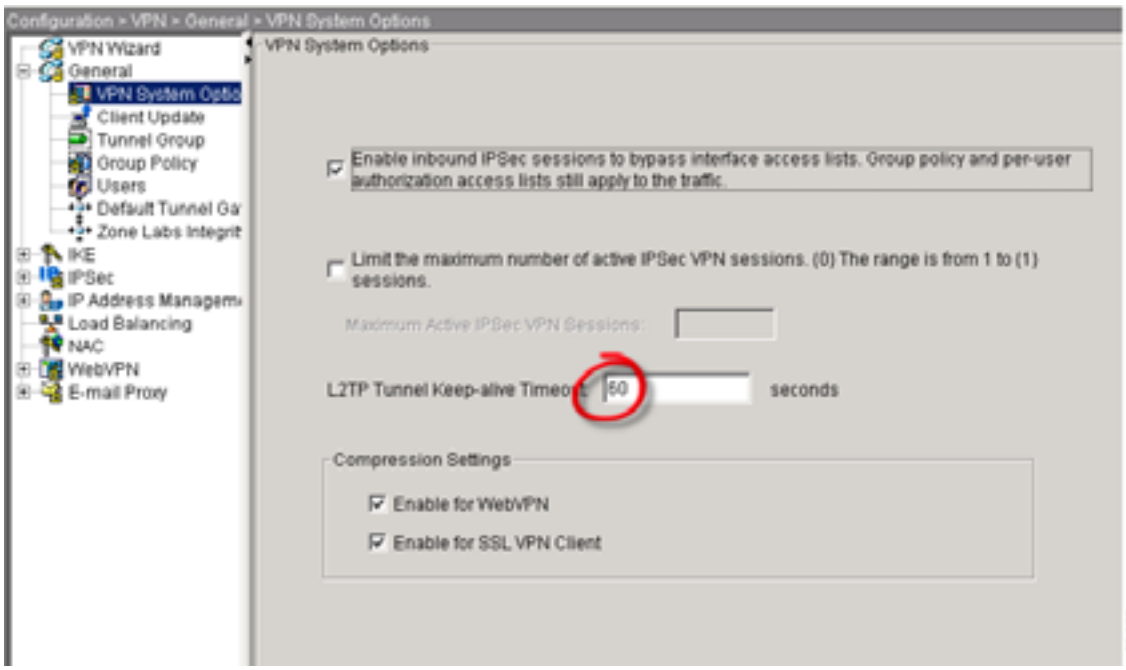
ユーザが Microsoft CHAP、バージョン 1 または 2 を使用する 2L2TP クライアントで、セキュリティ アプライアンスがローカル データベースに対して認証を行うように設定されている場合、**User Authenticated using MSCHAP** をクリックして MSCHAP を有効にする必要があります。

図 10-12　Add User Account ダイアログ



ステップ 9　hello　メッセージの間隔を秒単位で設定します。**VPN** > **Configuration** > **General** > **VPN System Options** を選択します。VPN System Options ペインが表示されます（図 10-13）。**L2TP Tunnel Keep-alive Timeout** フィールドに、値を秒単位で入力します。

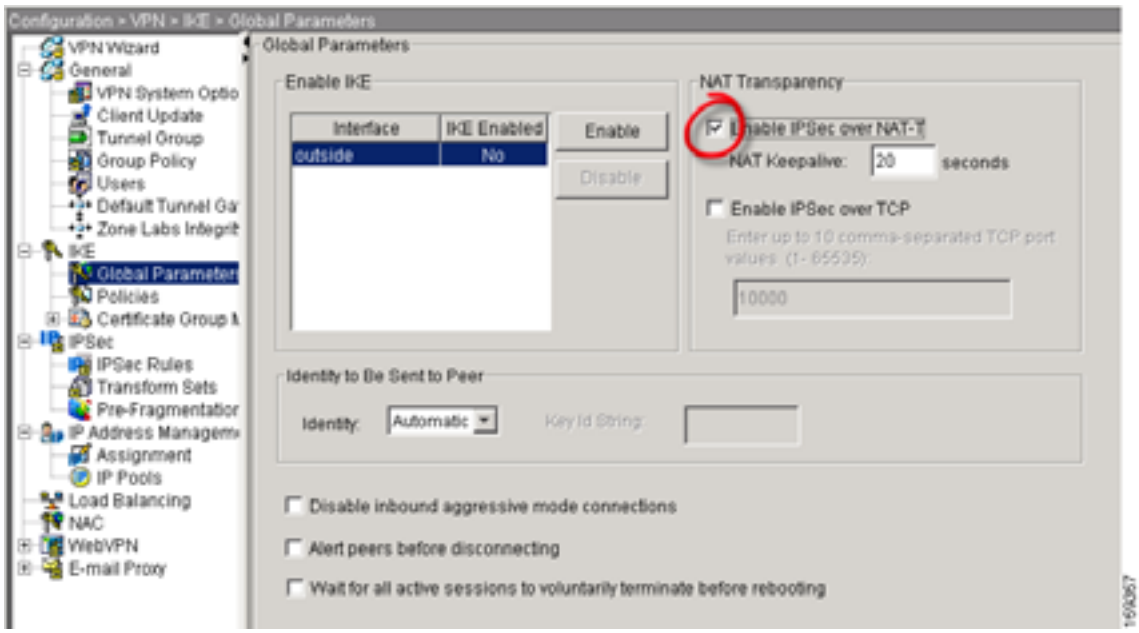
図 10-13　VPN System Options



ステップ 10（オプション）NAT デバイスの背後で、複数の L2TP クライアントが、セキュリティ アプライアンスへの L2TP over IPSec 接続を試みる可能性がある場合、ESP パケットが 1 つ以上の NAT デバイス経由で伝送されるように、NAT トラバーサルを有効にする必要があります。

これには、**Configuration > VPN > IKE > Global Parameters** を選択します。IKE Global Parameters ペインが表示されます（図 10-14）。インターフェイスで、ISAKMP が有効であることを確認します。**Enable IPSec over NAT-T** をオンにし、**OK** をクリックします。

図 10-14　IKE Global Parameters ペイン



CHAPTER 11

ロード バランシングの設定

この章では、ASDM を使用したロード バランシングの設定方法を説明します。この章には、次の項があります。

概要

リモート アクセス設定で、複数のセキュリティ アプライアンスまたは VPN コンセントレータが同じネットワークに接続されてリモート 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 バランシングを実装するには、同じプライベート LAN 間ネットワーク、プライベート サブネット、パブリック サブネットにある複数のデバイスを 1 つの仮想クラスタに論理的にグループ化します。

仮想クラスタ内のすべてのデバイスが、セッション負荷を分担します。ロード バランシングは、セッションのトラフィックをクラスタ内の最も負荷の小さいデバイスに割り当てることによって、すべてのデバイス間に負荷を分散します。これにより、システム リソースが効率的に利用でき、パフォーマンスと可用性が向上します。

仮想クラスタ マスターと呼ばれる仮想クラスタ内の 1 つのデバイスが、セカンダリ デバイスと呼ばれる残りのデバイスに着信トラフィックを割り当てます。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監視し、それぞれの作業負荷を追跡し、それに応じてセッション負荷を分散します。仮想クラスタ マスタの役割は、1 台の物理デバイスに固定されているのではなく、デバイス間で入れ替わることができます。たとえば、現在の仮想クラスタ マスターが故障すると、クラスタ内のセカンダリ デバイスの 1 つがその役割を引き継ぎ、即座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からは、単一の仮想クラスタ IP アドレスとして認識されます。この IP アドレスは、特定の物理デバイスに固定されているわけではありません。これは、現在の仮想クラスタ マスターに所属します。つまり、仮想アドレスです。VPN クライアントが接続を確立しようとするとき、この仮想クラスタ IP アドレスにまず接続します。すると仮想クラスタ マスターは、クラスタ内の最も負荷の小さい利用可能なホストのパブリック IP アドレスをそのクライアントに送り返します。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）。このように、仮想クラスタ マスターは、トラフィックを均一かつ効率的にリソース間に割り当てます。

(注) Cisco VPN Client、Cisco VPN 3002 Hardware Client、または Cisco ASA モデル 5505 以外のすべてのクライアントは、ハードウェア クライアントとして通常どおりセキュリティ アプライアンスに接続するよう設定されている場合は、仮想クラスタ IP アドレスを使用しません。

クラスタ内のマシンが故障してセッションが終了した場合、仮想クラスタ IP アドレスに即座に再接続できます。仮想クラスタ マスターは、次にこのような接続をクラスタ内の他のアクティブ デバイスに割り当てます。仮想クラスタ マスター自体が故障した場合、クラスタ内の他のデバイスが、即座に自動的に新しいセッション マスターになります。クラスタ内の複数のデバイスが故障した場合でも、クラスタ内のいずれか 1 つのデバイスが稼働し、利用可能である限り、ユーザは引き続きそのクラスタに接続できます。

ロード バランシングの実装

ロード バランシングを有効にするには、次の作業を行います。

- ロード バランシング クラスタの設定。共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタ用 IPSec 共有秘密鍵を確立します。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。
- 参加デバイスの設定。デバイス上でロード　バランシングを有効にし、デバイス固有のプロパティを定義します。これらの値は、デバイスによって異なります。

（注） VPN ロード バランシングには、アクティブな 3DES/AES ライセンスが必要です。セキュリティ アプライアンスは、ロード バランシングを有効にする前に、この暗号化ライセンスが存在するかをチェックします。アクティブな 3DES または AES ライセンスを検出しない場合、ライセンスによってこの使用が許可されない限り、セキュリティ アプライアンスは、ロードバランシングの有効化を阻止するとともに、ロード バランシングシステムによる 3DES の内部設定を阻止します。

前提条件

ロード バランシングは、デフォルトで無効です。ロード バランシングは明示的に有効にする必要があります。

まず、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とともに、仮想クラスタ IP アドレスの参照先の仮想クラスタ IP のインターフェイスをあらかじめ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、IP アドレス、暗号化設定、暗号化鍵、およびポートについて、クラスタ固有の値を共有する必要があります。

適格なプラットフォーム

ロード バランシング クラスタには、セキュリティ アプライアンス モデル ASA 5520 以上を使用できます。また VPN 3000 シリーズのコンセントレータも使用可能です。混合構成は可能ですが、一般に同種のクラスタの方が、管理が簡単です。

適格なクライアント

ロード バランシングは、次のクライアントが開始したリモート セッションでだけ有効です。

- Cisco VPN クライアント（リリース 3.0 以降）
- Cisco VPN 3002 ハードウェア クライアント（リリース 3.5 以降）
- Cisco ASA モデル 5505（ハードウェア クライアントとして設定した場合）
- Cisco PIX 501/506E（Easy VPN として動作する場合）

IPSec クライアントと WebVPN セッションの両方と連係して動作するロード バランシング LAN 間接続を含む他のすべてのクライアントは、ロード バランシングが有効なセキュリティ アプライアンスに接続することはできますが、ロード バランシングに参加することはできません。

VPN ロード バランシングのクラスタ設定

ロード バランシングクラスタは、すべての ASA リリース 7.0（x）セキュリティ アプライアンス、すべての ASA リリース 7.1（1）セキュリティ アプライアンス以降、すべての VPN 3000 コンセントレータ、またはこれらを組み合せて構成できます。次の制約があります。

- すべての ASA 7.0（x）セキュリティ アプライアンス、ASA 7.1（1）セキュリティ アプライアンス以降、またはすべての VPN 3000 コンセントレータで構成されるロード バランシング クラスタは、IPSec セッションと WebVPN セッションの組み合せに対してロード バランシングを実行できます。
- ASA 7.0（x）セキュリティ アプライアンスと VPN 3000 コンセントレータで構成されるロード バランシング クラスタは、IPSec セッションと WebVPN セッションの組み合せに対してロード バランシングを実行できます。
- ASA 7.1（1）セキュリティ アプライアンス以降と ASA 7.0（x）か VPN 3000 コンセントレータまたはその両方で構成されるロード バランシング クラスタは、IPSec セッションだけをサポートできます。ただしこのような構成では、ASA 7.1（1）以降のセキュリティ アプライアンスは最大の IPSec 能力を発揮できない場合もあります。P.11-5 の「シナリオ 1：WebVPN 接続のない混合クラスタ」に、この状況について示します。

リリース 7.1（1）以降では、クラスタ内の各デバイスの負荷の判定にあたって、IPSec セッションと WebVPN セッションの数や量が等しく測定されます。これは、ASA リリース 7.0（x）ソフトウェアと VPN 3000 コンセントレータのロード バランシング計算から大きく進歩した点です。これらの従来のプラットフォームでは、いずれも 1 つの WebVPN セッションを 10 の IPSec セッションと同じ負荷として計算する加重アルゴリズムを使用していました。

クラスタの仮想マスターは、セッション負荷をクラスタのメンバに割り当てます。ASA リリース 7.1（1）以降のセキュリティ アプライアンスは、すべてのセッション、Web VPN、IPSec、を等価と考え、そのように割り当てます。ASA リリース 7.0（x）セキュリティ アプライアンスまたは VPN 3000 コンセントレータは、セッション負荷の割り当てにおいて 10:1 の加重計算をします。

混合構成、つまりロード バランシング クラスタに、複数のリリースの ASA ソフトウェア、リリース 7.1（x）以降が動作する少なくとも 1 つのセキュリティ アプライアンス、および VPN 3000 コンセントレータが混在して動作している場合、最初のクラスタ マスターが故障して別のデバイスがマスターとして引き継いだときに、加重アルゴリズムの違いが問題となることがあります。

たとえば、ASA リリース 7.1（1）ソフトウェアが動作するセキュリティ アプライアンスが最初のクラスタ マスターであるとします。そしてそのデバイスが故障したとします。クラスタの別のデバイスが、自動的にマスターとして引き継ぎ、そのロード バランシング アルゴリズムを適用して、クラスタ内のプロセッサ負荷を判定します。しかし ASA リリース 7.1（1）ソフトウェアが動作するクラスタは、そのソフトウェアが提供する以外の方法で、セッション負荷を加重することができません。したがって、IPSec セッション負荷と WebVPN セッション負荷が混在している場合、旧バージョンが動作している ASA デバイスや VPN 3000 コンセントレータに対して、適切に負荷を割り当てられません。逆に、VPN 3000 コンセントレータがクラスタ マスターとして動作しているときは、ASA リリース 7.1（1）セキュリティ アプライアンスに負荷を適切に割り当てられません。P.11-5 の「シナリオ 2：WebVPN 接続を処理する混合クラスタ」にこのジレンマを示します。

（注） 許容される IPSec セッションと WebVPN セッションの数は、構成とライセンスによって許可される最大数まで設定できます。このような制限を設定する方法については、P.11-8 の「VPN セッション制限の設定」を参照してください。

混合クラスタのシナリオ

次のシナリオは、ASA リリース 7.1（1）以降、ASA リリース 7.0（x）ソフトウェア、VPN 3000 シリーズ コンセントレータがそれぞれ動作するさまざまなセキュリティ アプライアンスが混在するクラスタで、VPN ロード バランシングを使用する方法を示します。

シナリオ 1：WebVPN 接続のない混合クラスタ

このシナリオでは、クラスタにセキュリティ アプライアンスと VPN 3000 コンセントレータが混在しています。セキュリティ アプライアンス クラスタの中には、ASA リリース 7.0（x）が動作するデバイスもあれば、リリース 7.1（1）以降が動作するデバイスもあります。7.1（1）より前リリースと VPN 3000 のデバイスには、SSL VPN 接続機能がまったくなく、7.1（1）以降のリリースのデバイスは、基本の SSL VPN ライセンスしかありません。したがって、2 つの Web VPN セッションは設定できますが、SSL VPN 接続は利用できません。この場合、すべての接続が IPSec となり、ロード バランシングが適切に機能します。

2 つの WebVPN ライセンスは、ユーザが IPSec のセッション制限を最大限まで利用することに関してほとんど影響を及ぼしません。またその影響は VPN 3000 コンセントレータがクラスタ マスターの場合に限られます。一般に、IPSec セッションだけのシナリオでは、混合クラスタのセキュリティ アプライアンスにある Web VPN が少なければ少ないほど、ASA 7.1（1）以降のデバイスが IPSec のセッション制限に達する可能性が小さくなります。

シナリオ 2：WebVPN 接続を処理する混合クラスタ

このシナリオは、クラスタにセキュリティ アプライアンスと VPN 3000 コンセントレータが混在する上のシナリオと似ています。セキュリティ アプライアンス クラスタの中には、ASA リリース 7.0（x）が動作するデバイスもあれば、リリース 7.1（1）以降が動作するデバイスもあります。しかしこのケースでは、クラスタが IPSec 接続だけでなく、SSL VPN 接続も処理します。

ASA リリース 7.1（1）より前のソフトウェアが動作するデバイスがクラスタ マスターの場合、マスターが実際にはリリース 7.1（1）より前のプロトコルとロジックを適用することになります。つまり、そのセッション制限を超えているロード バランシング デバイスにセッションが割り当てられる可能性があります。この場合、ユーザはアクセスを拒否されます。

クラスタ マスターが、ASA リリース 7.0（x）ソフトウェアを実行するデバイスの場合、古いセッション加重アルゴリズムは、クラスタ内の 7.1（1）より前のデバイスにだけ適用されます。この場合、ユーザが拒否されることはありません。7.1（1）より前のデバイスはセッション加重アルゴリズムを使用するため、負荷が軽くなります。

ただし、クラスタ マスターが常に 7.1（1）以降のデバイスになることを保証できないという問題があります。クラスタ マスターが故障すると、他のデバイスがマスターの役割を引き継ぎます。新しいマスターには、適格なデバイスであれば、どれでもなれます。どのデバイスがマスターになるかを予見できないため、このタイプのクラスタ構成は避けることをお勧めします。

ロード バランシングの設定

ASA リリース 7.1（1）以降のソフトウェアが動作するセキュリティ アプライアンスでロード バランシングを設定するには、クラスタに参加する各デバイスに次の要素を設定します。

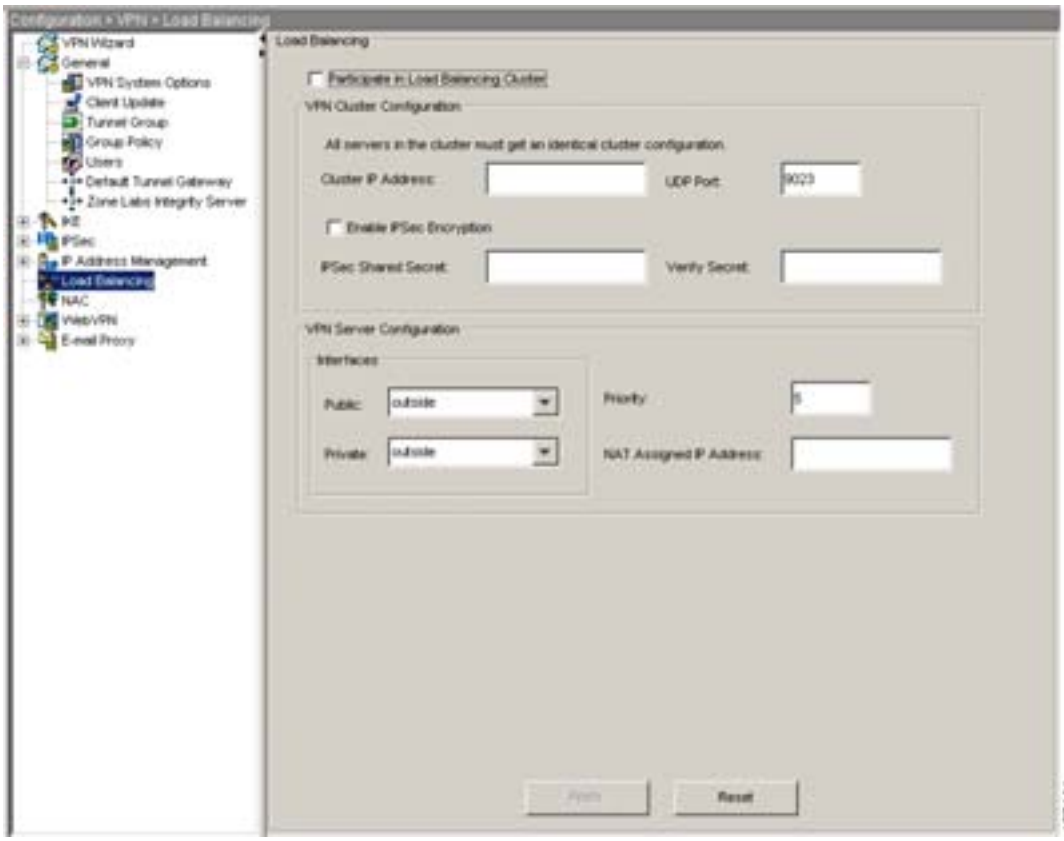
- パブリックとプライベートのインターフェイス
- VPN ロード バランシング クラスタ アトリビュート

（注） クラスタのすべての参加デバイスには、クラスタ内のデバイスの優先順位を除き、同一のクラスタ設定を行う必要があります。

ロード バランシングのパブリックとプライベートのインターフェイスの設定

ロード バランシング クラスタを設定するには、**Configuration > VPN > Load Balancing** を選択します（図 11-1）。

図 11-1　Load Balancing ウィンドウ



ロード バランシングを設定する手順は、次のとおりです。

ステップ 1　Participate in Load Balancing チェックボックスをオンにします。

ステップ 2　VPN Cluster Configuration 領域で次のようにアトリビュートを設定します。

（注）　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。

a. **Cluster IP Address** を入力します。これは、仮想クラスタ全体を表す単一の IP アドレスです。仮想クラスタ内のすべてのセキュリティ アプライアンス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。

b. **UDP Port** に、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がこのポートを使用している場合は、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。

c. オプションで、クラスタに対して IPSec の暗号化を有効にします。これには、**Enable IPSec Encryption** チェックボックスをオンにします。デフォルトでは、暗号化が無効です。このアトリビュートによって、IPSec の暗号化の有効と無効が切り替えられます。このアトリビュートを設定する場合、共有秘密鍵を指定し、確認する必要があります。仮想クラスタ内のセキュリティ アプライアンスは、IPSec を使用して LAN 間トンネル経由で通信を行います。デバイス間のすべてのロード バランシング情報が暗号化されるようにするには、この属性をオンにします。

（注）　暗号化を使用する場合は、ロード バランシングの内部インターフェイスをあらかじめ設定しておく必要があります。内部インターフェイスが有効でない場合は、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。

クラスタの暗号化を設定したときに、ロード バランシングの内部インターフェイスが有効でも、仮想クラスタのデバイスの参加を設定する前に無効にすると、Participate in Load Balancing Cluster チェックボックスを選択した時点でエラー メッセージが表示され、クラスタの暗号化を有効にできません。

d. クラスタの暗号化を有効にする場合は、IPSec の共有秘密鍵も指定する必要があります。これには、**IPSec Shared Secret** フィールドに値を入力してから、同じ値を **Verify Secret** フィールドに入力します。これらのフィールドには同一の値を設定する必要があります。これらのコマンドは、IPSec の暗号化を有効にしたときに、IPSec デバイス間の共有秘密鍵を指定します。このフィールドに入力した値は、一連のアスタリスクとして画面に表示されます。

ステップ 3　VPN Server Configuration 領域で次のようにアトリビュートを設定します。

a. **Public** で、セキュリティ アプライアンスのパブリック インターフェイスを選択します。このコマンドは、このデバイスのロード バランシングに使用するパブリック インターフェイスの名前または IP アドレスです。デフォルト値は outside です。

b. **Private** で、セキュリティ アプライアンスのプライベート インターフェイスを選択します。このコマンドは、このデバイスのロード バランシングに使用するプライベート インターフェイスの名前または IP アドレスです。デフォルト値は inside です。

c. クラスタ内でこのデバイスに割り当てる優先順位を設定します。範囲は 1 ～ 10 です。この優先順位は、このデバイスが、起動時または他のマスターの故障時に仮想クラスタ マスターになる可能性を示します。優先順位を高く設定すれば（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。

d. ネットワーク アドレス変換をこのデバイスに適用する場合は、NAT Assigned IP Address に、NAT に割り当てられた IP アドレスを入力します。

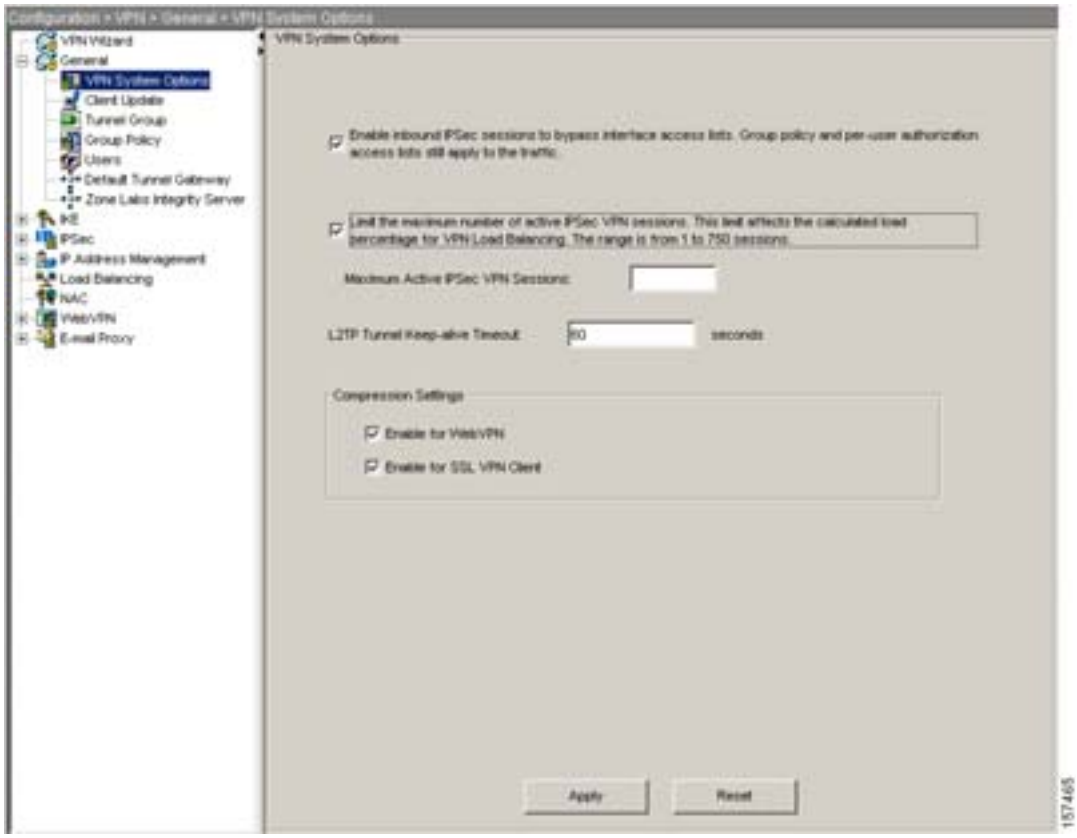
VPN セッション制限の設定

IPSec セッションと WebVPN セッションは、プラットフォームと セキュリティ アプライアンスのライセンスがサポートする限り、いくつでも実行できます。セキュリティ アプライアンスのライセンス情報を表示するには、ASDM の初期ウィンドウの上部にある Home アイコンを選択し、License タブを選択します（図 11-2）。

図 11-2　ライセンス情報

アクティブな IPSec VPN セッションの最大数を制限して、セキュリティ アプライアンスが許可している数より小さくするには、**Configuration > VPN > General > VPN System Options** を選択します（図 11-3）。

図 11-3　VPN System Options ウィンドウ



Maximum Active IPSec VPN Sessions フィールドに、適用する制限値を指定します。セッションの最大数は、ライセンスによって決まります。この制限は、VPN Load Balancing の負荷率の計算に影響を与えます。

たとえば、セキュリティ アプライアンス ライセンスが 750 の IPSec セッションを許可していて、IPSec セッション数を 500 に制限する場合は、**Maximum Active IPSec VPN Sessions** フィールドに 500 と入力します。

セッション制限を削除するには、**Limit the maximum number of active IPSec VPN sessions** チェックボックスをオフにします。

各種ライセンスで利用できる機能の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の付録 A「Feature Licenses and Specifications」を参照してください。

CHAPTER 12

ASA 5505 での Easy VPN Services の設定

この章では、ASDM を使用して ASA 5505 を Easy VPN ハードウェア クライアントとして設定する方法について説明します。この章の説明では、スイッチ ポートが設定され、ASA 5505 の VLAN インターフェイスが設定済みであると想定します（『*Cisco Security Appliance Command Line Configuration Guide*』の「Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance」を参照）。

(注) Easy VPN ハードウェア クライアントの設定では、そのプライマリ Easy VPN サーバとセカンダリ（バックアップ）Easy VPN サーバの IP アドレスを指定します。ASA は、ヘッドエンドとして設定されたもう 1 台の ASA 5505、VPN 3000 シリーズのコンセントレータ、IOS ベースのルータ、またはファイアウォールなど、どのような ASA でも Easy VPN サーバとして使用できます。ただし、1 台の ASA 5505 を同時にクライアント兼サーバとして使用することはできません。ASA 5505 をサーバとして設定する方法については、P.12-5 の「Cisco ASA 5505 の役割（クライアントまたはサーバ）の指定」を参照してください。次に、ASA 5505 を他の ASA と同様に設定します。これについては、『*Cisco Security Appliance Command Line Configuration Guide*』の「Getting Started」以降の章を参照してください。

この章には、次の項があります。

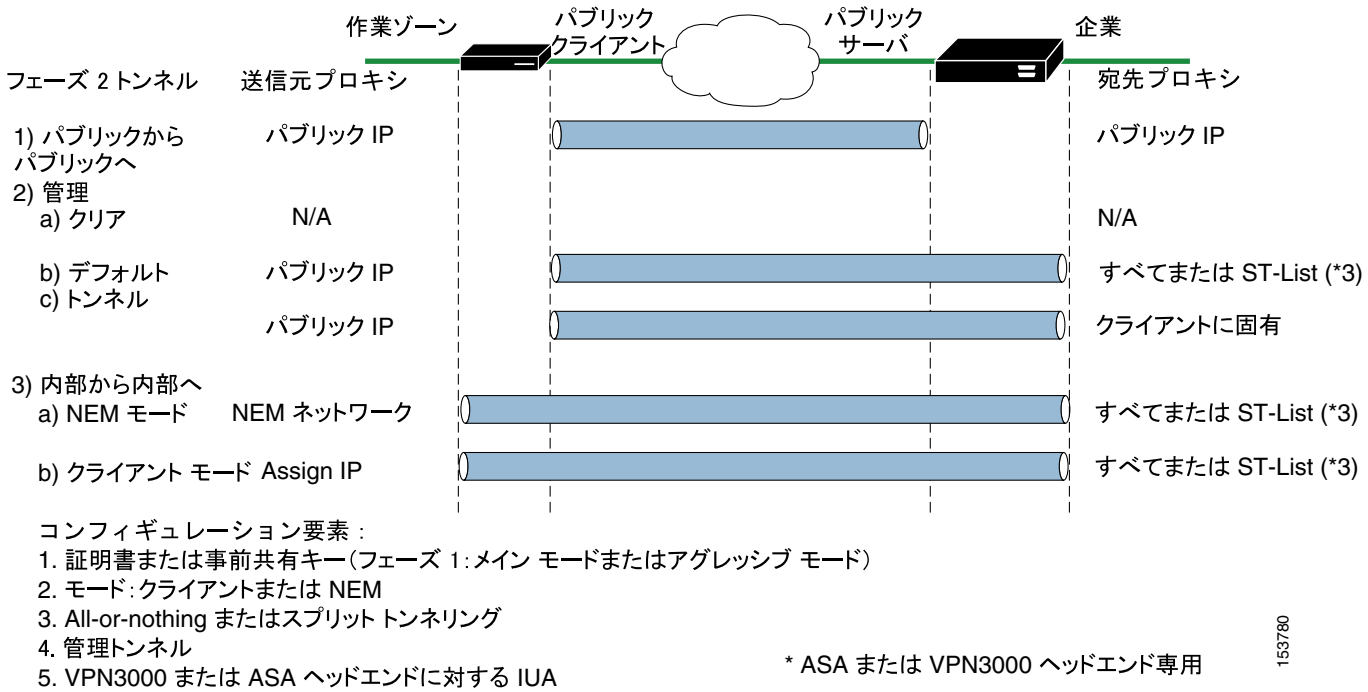
トンネリング オプションの比較

Easy VPN ハードウェア クライアントとして設定された Cisco ASA 5505 が設定するトンネル タイプは、次の要素によって異なります。

- Enable Tunneled Management アトリビュートを使用すると、データ トンネル以外にリモート管理用の IPSec トンネルを自動で確立できます。Clear Tunneled Management アトリビュートを使用すると、通常のルーティングを使用して管理アクセスが可能になります。またどちらのアトリビュートも使用しなければ、ヘッドエンド上でスプリット トンネリングを許可、制限、または禁止する Split Tunnel Policy アトリビュートまたは Split Tunnel Network List アトリビュートに従い、IPSec を使用して管理トンネルが設定されます（Enable Tunneled Management アトリビュートおよび Enable Tunneled Management アトリビュートの設定方法については、P.12-12 の「トンネル管理の設定」を参照してください。ヘッドエンド上で Split Tunnel Policy アトリビュートおよび Split Tunnel Network List アトリビュートを設定する方法については、P.2-32 の「クライアント設定パラメータの設定」を参照）。
- クライアント側から見て内部ホストを企業ネットワークまたはネットワーク拡張モードから隔離する Client Mode アトリビュートを使用すると、企業ネットワークからそれらのアドレスにアクセスできるようになります。

図 12-1 は、Easy VPN ハードウェア クライアントが、複数のアトリビュート設定に基づいて開始するトンネルのタイプを示します。

図 12-1　Cisco ASA 5505 の Easy VPN ハードウェア クライアントのトンネリング オプション



「All-or-nothing」という語は、スプリット トンネリングのアクセス リストが存在または不在であることを意味します。アクセス リストは、トンネリングが必要なネットワークと、必要でないネットワークを区別します。

はじめに（Easy VPN ハードウェア クライアントのみ）

ASA 5505 を Easy VPN ハードウェア クライアントとして設定する前に、次の手順を実行する必要があります。

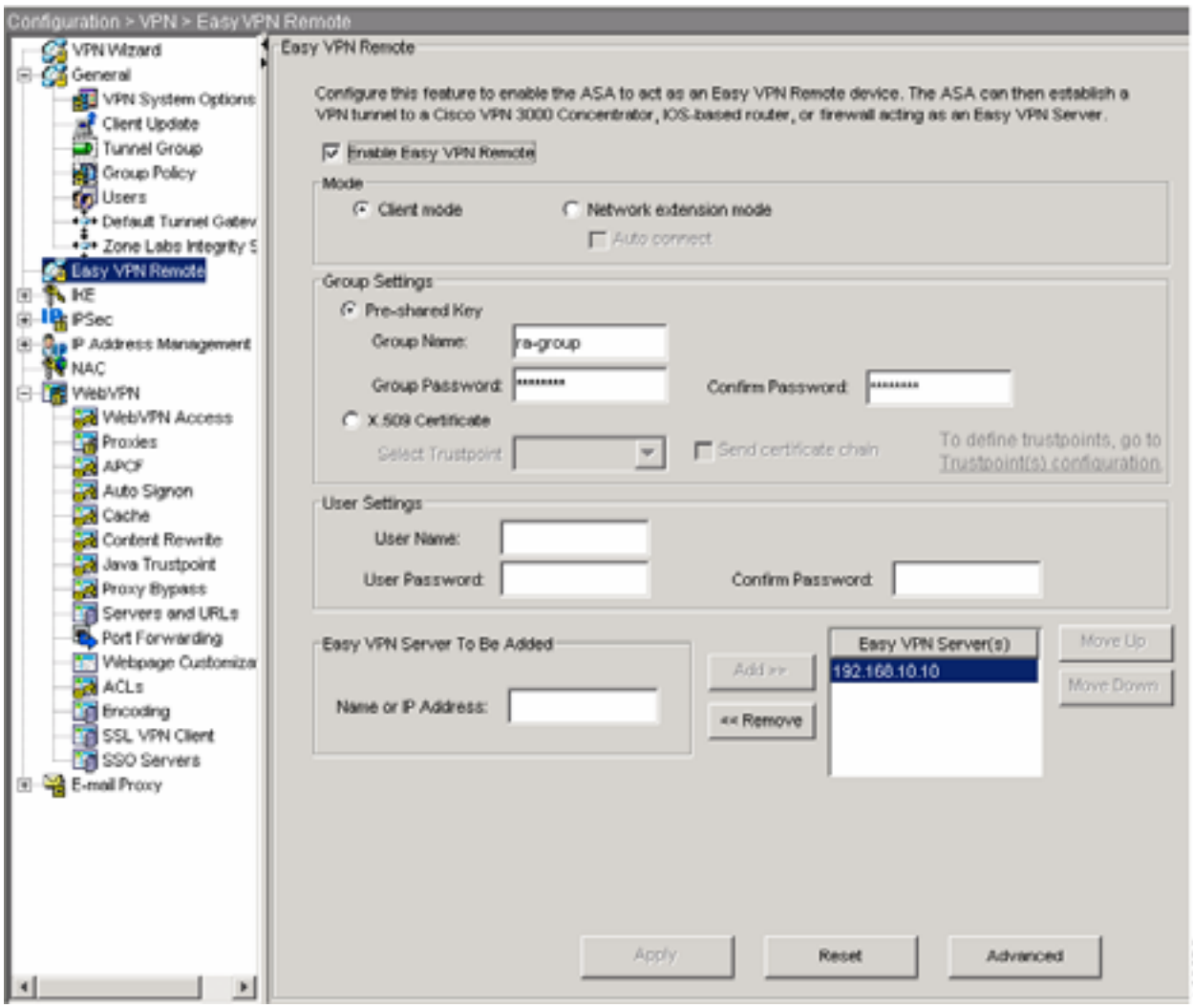
- サーバで必要な認証方式に応じて、次のいずれかの情報を取得します。
  - ヘッドエンドでの認証に事前共有鍵が必要な場合は、トンネルグループ名と事前共有鍵（グループ パスワード）。ヘッドエンドが ASA の場合、そのヘッドエンドに ASDM 接続すると、Configuration > VPN > General > Tunnel Group ウィンドウにトンネル グループ名が表示されます。トンネル グループ名をダブルクリックし、IPSec タブを開くと、事前共有鍵が表示されます。
  - ヘッドエンドでの認証にトラストポイントが必要な場合は、トラストポイント名と証明書チェーンの送信がアクティブかどうかを確認する必要があります。また、Easy VPN ハードウェア クライアントとして使用する ASA 5505 に、トラストポイントを設定する必要があります。ヘッドエンドが ASA の場合、そのヘッドエンドに ASDM 接続すると、Configuration > VPN > General > Tunnel Group > Add or Edit tunnel > IPSec タブにトラストポイント名と証明書チェーン インジケータが表示されます。次の手順に進む前に、P.1-4 の「トラストポイントの作成」の手順に従って、Easy VPN ハードウェア クライアントとして使用する ASA 5505 に、補助的なトラストポイントを設定する必要があります。
- （オプション）Easy VPN ハードウェア クライアントが、サーバからの IKE Extended Authenticate（Xauth; 拡張認証）チャレンジに対して使用するユーザ名とパスワードを取得します。
- Easy VPN サーバの役割を果たすプライマリとバックアップのヘッドエンドの IP アドレス。

基本設定の指定

Cisco ASA 5505 の基本設定では、それが Easy VPN ハードウェア クライアントとして機能するかどうか、また機能する場合は、内部ネットワーク上のホストの IP アドレスを、企業ネットワーク上のホストに公開するか隠蔽するか、ヘッドエンドへの接続の確立に使用されるグループまたはユーザ セキュリティ設定、および接続先のプライマリまたはバックアップ ヘッドエンドを指定します。

基本設定を行うには、Configuration > VPN > Easy VPN Remote を選択します。Easy VPN Remote ウィンドウが表示されます（図 12-2）。

図 12-2　Easy VPN Remote



以下の各項では、このウィンドウに表示される各アトリビュートに設定値を割り当てる方法を説明します。

Cisco ASA 5505 の役割（クライアントまたはサーバ）の指定

Cisco ASA 5505 は、Cisco Easy VPN ハードウェア クライアント（「Easy VPN Remote」）またはサーバ（「ヘッドエンド」）のいずれかとして動作し、同時に両方を兼ねることはできません。

ネットワークにおける ASA 5505 の役割は、次のように指定します。

ステップ 1　ASA 5505 をヘッドエンドとして設定した後、ハードウェア クライアントに変更する場合だけ、次のオブジェクトを削除または無効化します。

- ユーザ定義のトンネル グループをすべて削除するには、Configuration > VPN > General > Tunnel Group を選択し、デフォルト以外の各トンネル グループを選択して、**Delete**、**Apply** の順にクリックします。
- IPSec over TCP グローバル IKE 設定を無効にするには、Configuration > VPN > IKE > Global Parameters を選択し、IPSec over TCP をオフにして、**Apply** をクリックします。
- IKE ポリシーを削除するには、Configuration > VPN > IKE > Policies を選択し、各ポリシーを選択して、**Delete**、**Apply** の順にクリックします。
- IPSec ルールを削除するには、Configuration > VPN > IPSec > IPSec Rules を選択し、各ルールを選択して、**Delete**、**Apply** の順にクリックします。
- WebVPN を無効にするには、Configuration > VPN > WebVPN > WebVPN Access を選択し、各インターフェイスを選択して、**Disable**、**Apply** の順にクリックします。

（注）　設定の中でオブジェクト同士が競合する場合は、ASDM がエラー ウィンドウを表示するので、ASA 5505 を Easy VPN ハードウェア クライアント（以下のステップ 3 の「Easy VPN Remote」）として有効にし、Apply をクリックします。エラー ウィンドウには、設定の中に残っている、削除が必要なオブジェクトのタイプが表示され、これらを削除すると、Easy VPN Remote の設定値を設定に正常に保存できるようになります。

ステップ 2　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 3　次のどちらかを実行します。

- **Easy VPN Remote** をオンにして、ネットワークでの ASA 5505 の役割を Easy VPN ハードウェア クライアントとして指定します。
- **Easy VPN Remote** をオフにして、ネットワークでの ASA 5505 の役割をヘッドエンドとして指定します。

  このアトリビュートをオフにすると、その他のアトリビュートが淡色表示になります。

（注）　このアトリビュートをオフにした場合、**Apply** をクリックしてから、ASA 5505 を他の ASA と同様に設定します。これについては、『*Cisco Security Appliance Command Line Configuration Guide*』の「Getting Started」以降の章を参照してください。この章の残りの部分は無視してください。

User Settings 領域を除き、ASDM では、Easy VPN Remote をオンにした場合、このウィンドウのその他のアトリビュートを設定してから Apply をクリックする必要があります。以下の各項の説明に従ってこれらのアトリビュートを設定し、**Apply** をクリックして変更内容を実行コンフィギュレーションに保存します。

モードの指定

Easy VPN ハードウェア クライアントは、クライアント モードとネットワーク拡張モードの 2 つの操作モードのどちらかをサポートします。操作モードは、Easy VPN ハードウェア クライアントから見た内部ホストの IP アドレスが、企業ネットワークからトンネル経由でアクセス可能にするかどうかを指定します。Easy VPN ハードウェア クライアントにはデフォルト モードがないため、接続するには、その前に操作モードを指定しておくことが必要になります。

Easy VPN ハードウェア クライアントのモードを次のように指定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　次のいずれかのモード オプションをオンにします。

- **Client mode**：ポート アドレス変換（PAT）モードとも呼ばれます。クライアント モードでは、Easy VPN ハードウェア クライアントのプライベート ネットワークにあるすべてのデバイスが、企業ネットワークのデバイスから隔離されます。Easy VPN ハードウェア クライアントは、その内部ホストのすべての VPN トラフィックに対して PAT を実行します。

（注）　IP アドレス管理は、Easy VPN ハードウェア クライアントの内部インターフェイスについても、内部ホストについても必要ありません。

- **Network extension mode**（NEM）：内部インターフェイスおよびすべての内部ホストが、トンネル経由で企業ネットワークにルーティング可能になります。内部ネットワーク上のホストは、スタティック IP アドレスによって事前設定され、（スタティックにまたは DHCP 経由で）アクセス可能なサブネットから IP アドレスを取得します。PAT は、NEM 内の VPN トラフィックには適用されません。このモードでは、各クライアントに VPN 設定を行う必要はありません。NEM 用に設定された Cisco ASA 5505 は、自動トンネル起動をサポートします。設定には、グループ名、ユーザ名、パスワードを保存する必要があります。自動トンネル起動は、セキュアなユニット認証が有効な場合は無効になります。

  ASDM では、Network extension mode をオンにした場合にだけ、Auto connect チェックボックスがオンになります。

ステップ 3　Network extension mode をオンにした場合は、次の手順を実行します。

- **Auto connect**：Network extension mode がローカルに設定され、かつ Easy VPN Remote にプッシュされたグループ ポリシーでスプリットトンネリングが設定されている場合を除き、Easy VPN Remote は、自動 IPSec データ トンネルを確立します。両方の条件を満たしている場合は、このアトリビュートをオンにすると、IPSec データ トンネルの確立が自動化されます。両方の条件を満たしていて、このアトリビュートをオフにした場合、このアトリビュートは無視されます。

ステップ 4　Easy VPN Client の設定が完了し、Easy VPN Remote ウィンドウを開いて、Mode 領域のアトリビュートを変更し終わった場合にだけ、**Apply** をクリックします。そうでない場合は、Easy VPN Remote ウィンドウの残りのセクションを引き続き設定した後で、**Apply** をクリックします。

(注)　Easy VPN ハードウェア クライアントが NEM を使用し、セカンダリ サーバに接続されている場合は、各ヘッドエンドへの ASDM 接続を確立し、その ASDM 接続の Configuration > VPN > IPSec > IPSec Rules > Tunnel Policy (Crypto Map) - Advanced タブを開き、**Enable Reverse Route Injection** をオンにして、RRI を使用したリモート ネットワークのダイナミック アナウンスメントを設定します。

トンネル グループまたはトラストポイントの指定

Cisco ASA 5505 を Easy VPN ハードウェア クライアントとして設定する場合、Easy VPN サーバ上に設定された事前共有鍵またはトラストポイント名を指定できます。Easy VPN サーバとして使用するヘッドエンド上に設定し、認証に使用するオプションの名前の項を参照してください。

- 事前共有鍵の指定
- トラストポイントの指定

事前共有鍵の指定

次の手順に従って、ヘッドエンドの事前共有鍵に合わせて、Easy VPN ハードウェア クライアントの事前共有鍵を指定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　Group Settings の下の **Pre-shared Key** をクリックします。

以下は、このアトリビュートについての説明です。

- **Pre-shared key**：認証に IKE 事前共有鍵を使用することを指定します。このアトリビュートを指定すると、その後の、Group Name、Group Password、Confirm Password の各フィールドに、その鍵に含まれるグループ ポリシー名とパスワードを指定できるようになります。

ステップ 3　次のアトリビュートに値を割り当てます。

- **Group Name**：ヘッドエンド上に設定される VPN トンネル グループの名前。このトンネル グループは、接続を確立する前に、サーバ上に設定する必要があります。
- **Group Password**：ヘッドエンド上で認証に使用する IKE 事前共有鍵を入力します。

ステップ 4　Easy VPN Client の設定が完了し、Easy VPN Remote ウィンドウを開いて、グループ設定を変更し終わった場合にだけ、**Apply** をクリックします。そうでない場合は、P.12-8 の「自動 Xauth 認証の設定」以降の説明に従い、Easy VPN Remote ウィンドウの残りのセクションを引き続き設定した後で、**Apply** をクリックします。

トラストポイントの指定

次の手順に従って、ヘッドエンドに設定されているトラストポイントと、設定している Easy VPN ハードウェア クライアント上のそれに対応するトラストポイント（P.12-3 の「はじめに（Easy VPN ハードウェア クライアントのみ）」を参照）を指定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　このウィンドウの Group Settings 領域内の次のアトリビュートに値を割り当てます。

- **X.509 Certificate**：認証用に、認証局から提供された X.509 デジタル証明書の使用をクリックして指定します。
- **Select Trustpoint**：認証に使用する RSA 証明書を識別するトラストポイントを選択します。トラストポイント名には、IP アドレスの形式を使用できます。このドロップダウン リストに入力するトラストポイントを定義するには、右側の **Trustpoint(s) configuration** をクリックします。
- **Send certificate chain**：（オプション）証明書自体だけでなく、証明書チェーンの送信を有効にします。このアクションでは、ルート証明書と下位のすべての CA 証明書が送信されます。

ステップ 3　Easy VPN Client の設定が完了し、Easy VPN Remote ウィンドウを開いて、グループ設定を変更し終わった場合にだけ、**Apply** をクリックします。そうでない場合は、Easy VPN Remote ウィンドウの残りのセクションを引き続き設定した後で、**Apply** をクリックします。

自動 Xauth 認証の設定

次の条件がすべて満たされている場合、Easy VPN ハードウェア クライアントとして設定した ASA 5505 は、Easy VPN への接続時に自動的に認証を行います。

- セキュアなユニット認証が、サーバ上で無効になっている。
- サーバが IKE 拡張認証（Xauth）クレデンシャルを要求している。

  Xauth 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。Xauth は、RADIUS やその他のサポートされているユーザ認証プロトコルを使用して、ユーザ（この場合は、Easy VPN ハードウェア クライアント）を認証します。
- クライアント設定には、Xauth ユーザ名とパスワードが含まれています。

したがって、Easy VPN ハードウェア クライアントの Xauth ログイン クレデンシャルの設定はオプションです。

次のように、Xauth ログイン クレデンシャルを設定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　このウィンドウの Group Settings 領域内の次のアトリビュートに値を割り当てます。

- **User Name**：認証サーバまたはヘッドエンドからの Xauth チャレンジに対応して、Easy VPN ハードウェア クライアントが使用できるユーザ名を入力します。名前は、1 ～ 64 文字の間で、サーバまたはヘッドエンド上に設定する必要があります。

- **User Password**：認証サーバまたはヘッドエンドからの Xauth チャレンジに対応して、Easy VPN ハードウェア クライアントが使用できるパスワードを入力します。パスワードは、1 ～ 64 文字の間で、サーバまたはヘッドエンド上に設定する必要があります。
- **Confirm Password**：User Password に入力したユーザ パスワードを再度入力します。

ステップ 3　Easy VPN Client の設定が完了し、Easy VPN Remote ウィンドウを開いて、ユーザ設定を変更し終わった場合にだけ、**Apply** をクリックします。そうでない場合は、次の項に進んだ後で、**Apply** をクリックします。

Easy VPN サーバのアドレスの指定

Easy VPN ハードウェア クライアントとの接続を確立する前に、Easy VPN サーバとして動作するヘッドエンドの IP アドレスを少なくとも 1 つ指定する必要があります。ASA は、ヘッドエンドとして設定されたもう 1 台の ASA 5505、VPN 3000 シリーズのコンセントレータ、IOS ベースのルータ、またはファイアウォールなど、どのような ASA でも Easy VPN サーバとして使用できます。

プライマリの Easy VPN サーバと、バックアップとして使用する Easy VPN サーバの IP アドレスを次のように設定します。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択します。

Easy VPN Remote ウィンドウが表示されます（図 12-2）。

ステップ 2　次のアトリビュートの説明に従って、このウィンドウの Easy VPN Server To Be Added 領域に値を割り当てます。

Name or IP Address：プライマリ Easy VPN として使用するヘッドエンドの IP アドレスまたは DNS 名を入力し、**Add** をクリックします。この値は、ASDM の Easy VPN Server(s) リストに挿入されます。すべてのバックアップ Easy VPN サーバに対して、この操作を繰り返します。

ステップ 3　エントリを選択し、**Move Up** または **Move Down** をクリックして、関連付けられた Easy VPN サーバへの接続を試みる優先順位を設定します。

ステップ 4　関連付けられた Easy VPN サーバをリストから削除する場合は、エントリを選択して **Remove** をクリックします。

ステップ 5　**Apply** をクリックし、ウィンドウで行った変更を実行コンフィギュレーションに保存します。

（注）　エラー ウィンドウによって、Easy VPN ハードウェア クライアントとしての ASA 5505 の設定と競合するオブジェクトが識別された場合は、ASDM セッションがウィンドウの設定を保持します。エラー ウィンドウには、設定の中に残っている、削除が必要なオブジェクトのタイプが表示され、これらを削除すると、このウィンドウに変更を正常に保存できるようになります。競合するオブジェクトを削除した後、このウィンドウに戻って **Apply** を再度クリックします。

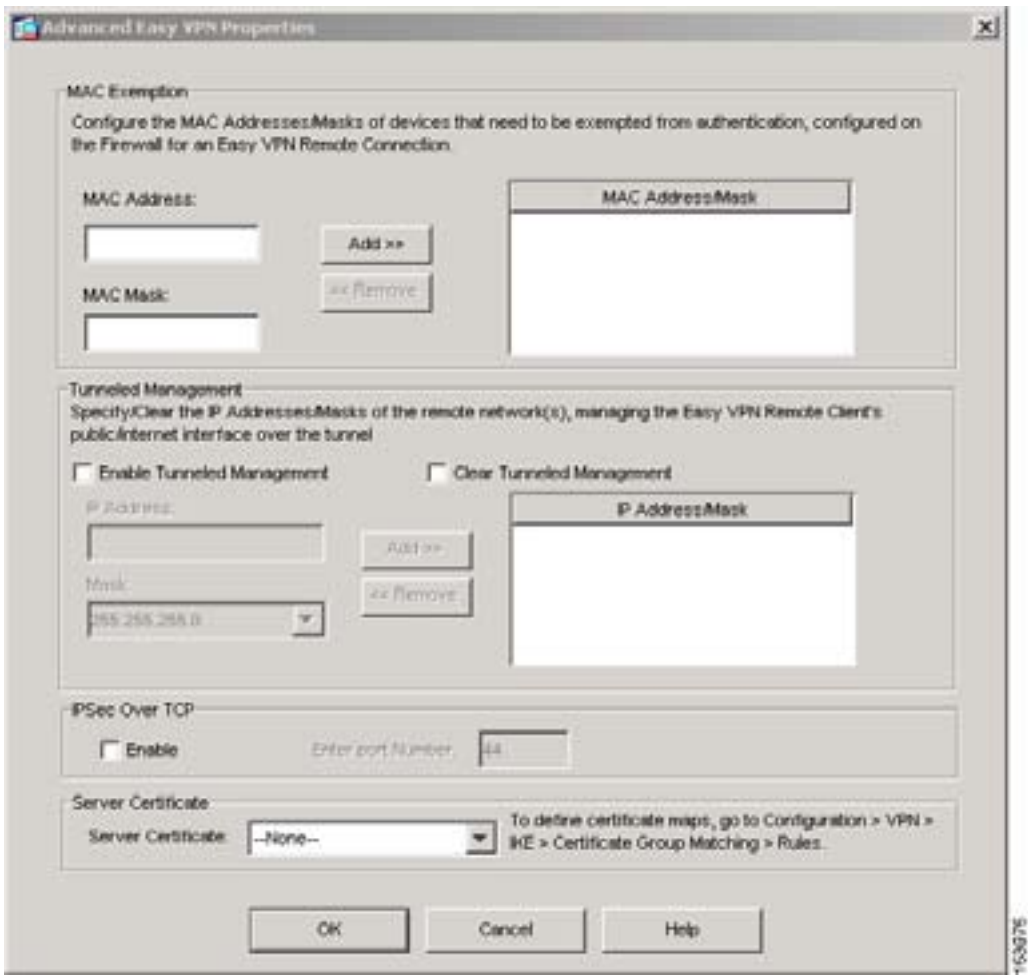
詳細設定の指定

Easy VPN ハードウェア クライアントの詳細設定はオプションです。次の設定が可能です。

- 内部ネットワーク上のデバイスを指定して、個別のユーザ認証を免除する。
- IPSec トンネルを自動的に作成して、企業ネットワークから ASA 5505 の外部インターフェイスへの管理アクセスを提供する。
- IPSec の TCP カプセル化の有効化と無効化。
- 証明書マップを指定し、その証明書マップが識別するデジタル証明書を持つ Easy VPN サーバにだけ、Easy VPN ハードウェア クライアントが接続を許可するように設定します。

Easy VPN ハードウェア クライアントの詳細設定を行うには、Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下の **Advanced** をクリックします。Advanced Easy VPN Remote Properties ウィンドウが表示されます（図 12-3）。

図 12-3　Advanced Easy VPN Remote Properties



（注）　各領域はオプションで、他の領域から互いに独立しています。このウィンドウの 1 つの領域を設定しても、別の領域を設定する必要は生じません。

以下の各項では、このウィンドウの各アトリビュートに設定値を割り当てる方法を説明します。

デバイス パススルーの設定

Cisco IP Phone、ワイヤレス アクセス ポイント、プリンタなどのデバイスは、認証を実行できません。個々のユーザ認証が有効な場合、次の手順に従って、デバイスをユーザ認証から除外し、そのデバイスにネットワーク アクセスを提供できます。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下部で **Advanced** をクリックします。

Advanced Easy VPN Remote Properties ウィンドウが表示されます（図 12-3）。このウィンドウ上部の MAC Exemption 領域では、デバイス パススルーを設定できます。

ステップ 2　次のアトリビュートに値を割り当てます。

- **MAC Address**：個々のユーザ認証をバイパスするデバイスの MAC アドレスを、ドット付き 16 進数表記で入力します。
- **MAC Mask**：MAC アドレスに対応するネットワーク マスクを入力します。ffff.ff00.0000 という MAC マスクは、同じ製造元が製造したすべてのデバイスに相当します。ffff.ffff.ffff という MAC マスクは、1 つのデバイスに相当します。

（注）　MAC マスク ffff.ff00.0000 を入力して、同じ製造元のすべてのデバイスを指定する場合、MAC アドレスの最初の 6 文字を入力するだけで済みます。たとえば、Cisco IP phones の製造元 ID が 00036b の場合、MAC アドレスとして `0003.6b00.0000` を入力し、MAC マスク コマンドとして `ffff.ff00.0000` を入力すると、将来追加する Cisco IP phone を含むすべての Cisco IP phone が認証を免除されます。MAC アドレス `0003.6b54.b213` と MAC マスク `ffff.ffff.ffff` を入力することでセキュリティは強化されますが、特定の 1 台の Cisco IP phone の認証を免除するため、柔軟性は低くなります。

ステップ 3　**Add** をクリックします。

MAC Address/Mask リストに MAC アドレスと MAC マスクが挿入されます。

ステップ 4　ユーザ認証を免除するデバイスが他にあれば、それぞれに対してステップ 2 と 3 を繰り返します。

ステップ 5　デバイスをリストから削除する場合は、エントリを選択して **Remove** をクリックします。

ステップ 6　Advanced Easy VPN Properties ウィンドウで他に変更するアトリビュートがない場合は、**OK**、**Apply** の順にクリックします。他に変更するアトリビュートがある場合は、次のセクションに進みます。

トンネル管理の設定

Cisco ASA 5505 は、Easy VPN ハードウェア クライアントとして動作するだけでなく、SSH または HTTPS を使用して、第 2 レイヤの追加暗号機能付きの、またはこの機能のない管理アクセスをサポートします。Easy VPN ハードウェア クライアントを設定することによって、管理セッションにすでに存在する IPSec 暗号化を SSH または HTTPS 暗号内で要求できます。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下部で **Advanced** をクリックします。

Advanced Easy VPN Remote Properties ウィンドウが表示されます（図 12-3）。

ステップ 2　次のいずれかのオプションを選択します。

- **Enable Tunneled Management**：オンにすると、IPSec トンネルを自動作成して、企業ネットワークから ASA 5505 の外部インターフェイスへの管理アクセスを提供します。Easy VPN ハードウェア クライアントとサーバは、データ トンネルの作成時に管理トンネルを自動的に作成します。
- **Clear Tunneled Management**：オンにすると、通常のルーティングを使用して、企業ネットワークから ASA 5505 の外部インターフェイスへの管理アクセスを提供します（管理パケットの非トンネリング）。このアトリビュートは、NAT デバイスが Easy VPN ハードウェア クライアントとインターネット間で動作している場合にオンにします。
- **Enable Tunneled Management** と **Clear Tunneled Management** の両方のチェックボックスをオフのままにすると、**split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って、管理トンネルの IPSec が設定されます。

（注）　ステップ 3 ～ 6 を使用するのは、Enable Tunneled Management をオンにした場合だけです。

ステップ 3　説明に従って、次のアトリビュートに値を割り当てます。

- **IP Address**：管理アクセス用の IPSec トンネルを自動作成するリモート ネットワークまたはホストの IP アドレスを入力します。
- **Mask**：入力した IP アドレスのサブネット マスクを選択します。

ステップ 4　**Add** をクリックします。

IP Address/Mask リストに IP アドレスとマスクが挿入されます。

ステップ 5　これ以外のネットワークまたはホストについて、リモート管理アクセス用の IPSec トンネルを自動作成する場合は、それぞれに対してステップ 3 と 4 を繰り返します。

ステップ 6　デバイスをリストから削除する場合は、エントリを選択して **Remove** をクリックします。

ステップ 7　Advanced Easy VPN Properties ウィンドウで他に変更するアトリビュートがない場合は、**OK**、**Apply** の順にクリックします。他に変更するアトリビュートがある場合は、次のセクションに進みます。

IPSec over TCP の設定

デフォルトで、Easy VPN ハードウェアとサーバは、IPSec を UDP（User Datagram Protocol）パケットにカプセル化します。特定のファイアウォール ルールや、NAT、PAT がある環境など、一部の環境では、UDP が使用できません。このような環境で標準の Encapsulating Security Protocol（ESP、Protocol 50）やインターネット キー エクスチェンジ（IKE、UDP 500）を使用するには、TCP パケット内にこれらのパケットをカプセル化してセキュアなトンネリングを行えるように、クライアントとサーバを設定する必要があります。ただし、使用している環境で UDP が利用できる場合は、IPSec over TCP を設定するのは不要なオーバーヘッドを追加するだけです。

IPSec の TCP カプセル化は、次のように有効または無効にします。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下部で **Advanced** をクリックします。

Advanced Easy VPN Remote Properties ウィンドウが表示されます（図 12-3）。

ステップ 2　次の説明に従って、IPSec Over TCP 領域のアトリビュートを設定します。

- **Enable (IPSec Over TCP)**：オンにすると、TCP を使用して IPSec over UDP パケットがカプセル化されます。オフにすると、UDP だけが使用されます。

  このアトリビュートをオンにすると、Enter port Number ボックスがアクティブになります。
- **Enter port Number**：IPSec over TCP に使用するポート番号を入力します。デフォルトで、Easy VPN ハードウェア クライアントは、ポート 10000 を使用しますが、Enable (IPSec Over TCP) をオンにした場合は、ポート番号を入力する必要があります。10000 を入力するか、ヘッドエンドに割り当てたものと同じポート番号を使用します。

ステップ 3　Advanced Easy VPN Properties ウィンドウで他に変更するアトリビュートがない場合は、**OK**、**Apply** の順にクリックします。他に変更するアトリビュートがある場合は、次のセクションに進みます。

（注）　Easy VPN Remote 接続で、TCP でカプセル化された IPSec を使用する場合は、Configuration > VPN > IPSec > Pre-Fragmentation を選択し、外部インターフェイスをダブルクリックし、DF Bit Setting Policy を Clear に設定します。この処理によって、Don't Fragment（DF）ビットが、カプセル化されたヘッダーからクリアされます。DF ビットは IP ヘッダーの中にあり、パケットのフラグメントが可能かどうかを決定します。このコマンドを使用すると、Easy VPN ハードウェア クライアントは、MTU のサイズを超えるパケットを送信できます。

証明書のフィルタリングの設定

証明書マップを指定し、その証明書マップが識別するデジタル証明書を持つ Easy VPN サーバにだけ、Easy VPN ハードウェア クライアントが接続を許可するように設定できます。それを設定するには、その前に Configuration > VPN > IKE > Certificate Group Matching > Rules メニュー パスを使用して、マップを作成する必要があります。その後、次の手順で証明書マップを割り当てます。

ステップ 1　Configuration > VPN > Easy VPN Remote を選択し、Easy VPN Remote ウィンドウの下部で **Advanced** をクリックします。

Advanced Easy VPN Remote Properties ウィンドウが開きます（図 12-3）。

ステップ 2　次の説明に従って、ウィンドウの下部でアトリビュートを設定します。

- **Server Certificate**：Easy VPN ハードウェア クライアント接続でサポートする証明書の識別に使用する証明書マップを選択します。Configuration > VPN > IKE > Certificate Group Matching > Rules メニュー パスを使用して Rules ウィンドウにアクセスすると、最初のテーブルのマッピング名が、ドロップダウン リストに表示されます。

ステップ 3　**OK**、**Apply** の順にクリックします。

Easy VPN サーバの設定のためのガイドライン

次の各項では、Easy VPN サーバに適用される Easy VPN ハードウェア クライアントについての考慮事項を説明します。

認証オプション

ASA 5505 は、次の認証メカニズムをサポートします。この認証メカニズムは、Easy VPN サーバに格納されているグループ ポリシーから取得されます。次のリストは、Easy VPN ハードウェア クライアントによってサポートされている認証オプションですが、これらは Easy VPN サーバ上で設定が必要です。

- Configuration > VPN General > Group Policy > Add or Edit Internal Group Policy > Hardware Client タブの Require Interactive Client Authentication （セキュアなユニット認証とも呼ばれます）

  このアトリビュートを有効にすると、Xauth ログイン クレデンシャル（P.12-8 の「自動 Xauth 認証の設定」を参照）が無視され、ユーザがパスワードを入力して ASA 5505 を認証する必要があります。
- 同じ Hardware Client タブの Require Individual User Authentication

  このアトリビュートを有効にすると、企業 VPN ネットワークにアクセスする前に、ASA 5505 を使用しているユーザが認証される必要があります。

注意　クライアントが NAT デバイスを持っている可能性がある場合は、IUA を使用しないでください。

- 同じ Hardware Client タブの User Authentication Idle Timeout

  このアトリビュートは、Easy VPN Server がクライアントのアクセスを終了するまでのアイドル タイムアウト期間を設定または解除します。
- Authentication by HTTP redirection

  次のいずれかの場合、Cisco Easy VPN サーバは、HTTP トラフィックを代行受信して、ユーザをログイン ページにリダイレクトします。

  — SUA またはユーザ名とパスワードが Easy VPN ハードウェア クライアント上に設定されていない場合

  — IAU が有効な場合

  HTTP リダイレクションは自動的に行われるため、Easy VPN サーバ上で設定する必要はありません。
- 事前共有鍵、デジタル証明書、トークン、無認証

  ASA 5505 は、ユーザ認証方式として、事前共有鍵、トークンベース（たとえば、SDI ワンタイム パスワード）、および「ユーザ認証なし」をサポートします。**注**：Cisco Easy VPN サーバは、ユーザ認証の一部として、デジタル証明書を使用できます。使用方法については、P.1-1 の「デジタル証明書の登録」を参照してください。

クライアントにプッシュされるグループ ポリシーとユーザ アトリビュート

トンネル確立時に、Easy VPN サーバは、その設定に格納されているグループ ポリシーまたはユーザ アトリビュートの値を Easy VPN ハードウェア クライアントにプッシュします。したがって、Easy VPN ハードウェア クライアントで使用されている一部のアトリビュートを変更するには、プライマリとセカンダリ Easy VPN サーバとして設定されているセキュリティ アプライアンス上でそれらのアトリビュートを変更する必要があります。この項では、Easy VPN ハードウェア クライアントにプッシュされるグループ ポリシー アトリビュートを示します。

(注)　この項は、参考資料として使用してください。グループ ポリシーの設定方法については、P.2-1 の「グループ ポリシーの設定」を参照してください。

Easy VPN サーバ上で変更が必要なグループ ポリシー アトリビュートについては、表 34-2 を参照してください。

表 12-1　EasyVPN ハードウェア クライアントとして設定された Cisco ASA 5505 にプッシュされるグループ ポリシーとユーザ アトリビュート

ASDM Group Policy タブ	アトリビュート	説明
General	Tunneling Protocols	許可されるトンネリング プロトコルを指定します。
General	Filter	VPN トラフィックに適用されます。
General	Access Hours	VPN のアクセス時間を制限します。
General	Simultaneous Logins	同時ログインの最大数を指定します。
General	Maximum Connect Time	VPN 接続の最大分数を指定します。
General	Idle Timeout	セッションがタイムアウトになるまでのアイドル時間を指定します。
General	DNS Servers	プライマリおよびセカンダリ DNS サーバの IP アドレスを指定するか、DNS サーバの使用を禁止します。
General	WINS Servers	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定するか、WINS サーバの使用を禁止します。
General	DHCP Scope	このグループ内で、DHCP サーバがユーザにアドレスを割り当てる IP サブネットワークを指定します。
IPSec	Re-authentication on IKE Re-key	IKE 鍵の再生成時に、Xauth 認証が必要です。 **注**：セキュアなユニット認証が有効な場合は、XAUTH 再認証を無効にします。
IPSec	Perfect Forward Security	VPN クライアントが、perfect forward secrecy（PFS; 完全転送秘密）を使用します。
IPSec	Tunnel Group Lock	トンネル グループによって、ユーザがそのグループに確実に接続されるよう指定します。
IPSec	Client Access Rules	アクセス ルールを適用します。
Client Configuration > General Client Parameters	Banner	トンネル確立後、クライアントにバナーを送信します。
Client Configuration > General Client Parameters	Default Domain	ドメイン名をクライアントに送信します。
Client Configuration > General Client Parameters	Split Tunnel DNS Names	名前解決のためにドメインのリストをプッシュします。

表 12-1　EasyVPN ハードウェア クライアントとして設定された Cisco ASA 5505 にプッシュされるグループ ポリシーとユーザ アトリビュート（続き）

ASDM Group Policy タブ	アトリビュート	説明
Client Configuration > General Client Parameters	Split Tunnel Policy	リモートアクセスの IPSec クライアントが、条件に応じて、パケットを暗号化して IPSec トンネル経由で送信するか、クリアテキストでネットワーク インターフェイスに送信します。オプションは次のとおりです。 • split-tunnel-policy：トンネリング トラフィックのルールを設定していることを示します。 • excludespecified：トラフィックがクリアテキストで送信されるネットワークのリストを定義します。 • tunnelall：クリアテキストで送信するトラフィックも、Easy VPN サーバ以外の宛先に送信するトラフィックも存在しないことを指定します。リモート ユーザは、企業ネットワーク経由でインターネット ネットワークに接続し、ローカル ネットワークにアクセスできません。 • tunnelspecified：指定されたネットワークとの間で送受信されるすべてのトラフィックをトンネリングします。このオプションによって、スプリット トンネリングが有効になります。またトンネルするアドレスのネットワーク リストが作成できます。他のすべてのアドレスに送信されるデータはクリアテキスト形式を取り、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。
Client Configuration > General Client Parameters	Split Tunnel Network List	次のどちらかを指定します。 • スプリット トンネリングのアクセスリストが存在しません。すべてのトラフィックは、トンネル経由で送信されます。 • トンネリングが必要なネットワークと、必要でないネットワークを、セキュリティ アプライアンスが区別するためのアクセス リストを指定します。 スプリット トンネリングでは、リモートアクセスの IPSec クライアントが、条件に応じて、パケットを暗号化して IPSec トンネル経由で送信するか、クリアテキストでネットワーク インターフェイスに送信します。スプリット トンネリングを有効にすると、IPSec トンネルの他端にある宛先以外に送信されるパケットは、暗号化され、トンネル経由で送信され、復号化され、最終宛先にルーティングされます。
Client Configuration > Cisco Client Parameters	Store Password on Client System	VPN ユーザがパスワードをユーザ プロファイルに保存できます。
Client Configuration > Cisco Client Parameters	IPSec over UDP	IPSec トンネルに UDP カプセル化を使用します。
Client Configuration > Cisco Client Parameters	IPSec over UDP Port	IPSec over UDP のポート番号を指定します。
Client Configuration > Cisco Client Parameters	IPSec Backup Servers	プライマリ サーバが応答できない場合に備えて、クライアント上にバックアップ サーバを設定します。
Client Firewall	（このタブ上のすべて）	VPN クライアント上に、ファイアウォール パラメータを設定します。
Hardware Client	Require Interactive Client Authentication	VPN ハードウェア クライアントで、セキュアなユニット認証を有効にします。

表 12-1　EasyVPN ハードウェア クライアントとして設定された Cisco ASA 5505 にプッシュされるグループ ポリシーとユーザ アトリビュート（続き）

ASDM Group Policy タブ	アトリビュート	説明
Hardware Client	Require Individual User Authentication	ハードウェアベースの VPN クライアントで、個別のユーザ認証を有効にします。
Hardware Client	Allow Network Extension Mode	ネットワーク拡張モードを有効または無効にします。

（注）　IPSec NAT-T 接続は、Cisco ASA 5505 の ホーム VLAN 上でサポートされている唯一の IPSec 接続タイプです。IPSec over TCP とネイティブな IPSec 接続はサポートされていません。

A

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

あ

い

お

か

き

く

こ

さ

し

す

せ

た

つ

て

と

な

に

ね

は

ふ

へ

ほ

ま

ゆ

り

ろ