選択したユーザ管理タスクの実行

この章では、VPN 3000 Concentrator Manager の User Management セクションで設定可能な、いくつかの ASA ユーザ管理機能を設定する方法について説明します。ASA では、以前は基本グループ、グループ、およびユーザ アトリビュートとして設定できたすべての機能を、グループ ポリシーとトンネル グループを使用して設定できます。

この章では、次のユーザ管理タスクについて説明します。

- スプリット トンネリングおよびネットワーク リストの設定
- クライアント ファイアウォールおよび VPN の設定
- 外部サーバを使用する認証

（注） ASDM には、完全なオンラインヘルプ システムが付属しています。パネルのフィールド定義を参照する場合は、**Help** をクリックしてください。
この章で使用するコマンドの完全なシンタックスについては、『*Cisco Security Appliance Command Reference*』を参照してください。

スプリット トンネリングおよびネットワーク リストの設定

スプリット トンネリングは、IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにするものです。IPSec トンネルの反対側の宛先にバインドされていないパケットについては、暗号化してからトンネルを介して送信し、復号化してから最終的な宛先にルーティングする必要はありません。このように、スプリット トンネリングを使用すると、トラフィックの管理が簡単になり、処理負荷が軽減されます。

スプリット トンネリングは、単一ユーザのリモート アクセス IPSec トンネルにだけ適用されます。LAN 間の接続には適用されません。

スプリット トンネリングは、基本的にトラフィック管理機能であり、セキュリティ機能ではありません。実際のところ、最適のセキュリティを得るには、スプリット トンネリングをイネーブルにしないことをお勧めします。しかし、スプリット トンネリングをイネーブルにできるのはセキュリティ アプライアンスだけで、IPSec クライアントはイネーブルにできないので、実装を制御することによりセキュリティを保護できます。デフォルトでは、スプリット トンネリングはセキュリティ アプライアンスおよび IPSec クライアントの両方でディセーブルです。この機能を ASA でイネーブルにして設定すると、機能は ASA により ISAKMP を介して IPSec クライアントにプッシュされ、IPSec クライアントでイネーブルにされます。

この項のコマンド例は、CLI で access-list コマンドを使用するか、ASDM で ACL Manager を使用することによって、ネットワーク リストを設定する方法を示しています。また、ネットワーク リストを使用するスプリット トンネリング用の内部グループ ポリシーを設定する方法と、グループ ポリシーを使用するリモート アクセス トンネル グループを設定する方法も示しています。

コンフィギュレーション手順の概要

スプリット トンネリングを設定する手順は、次のとおりです。

1. 標準のアクセス リストを使用してネットワーク リストを定義します。
2. スプリット トンネリング グループ ポリシーを作成するか、既存のリモート アクセス グループ ポリシーを変更します。
3. スプリット トンネリング用のトンネル グループを作成します。

この項の手順では、次のシナリオを使用します。

- ネットワーク リストの名前は split。
- グループ ポリシーの名前は splitgroup。
- トンネル グループの名前は splittunnel。
- トンネル グループ タイプは IPSec_RA。
- トンネル グループでは、認証に事前共有鍵を使用する。

次に例を示します。

```
hostname(config)# access-list split standard permit 172.16.1.0 255.255.255.0
hostname(config)# access-list split standard permit 192.168.1.0 255.255.255.0
hostname(config)# group-policy splitgroup internal
hostname(config)# group-policy splitgroup attributes
    hostname(config-group-policy)# split-tunnel-policy tunnelspecified
    hostname(config-group-policy)# split-tunnel-network-list value split
hostname(config)# tunnel-group splittunnel type ipsec_ra
hostname(config)# tunnel-group splittunnel general-attributes
    hostname(config-general)# default-group-policy splitgroup
hostname(config)# tunnel-group splittunnel ipsec-attributes
    hostname(config-ipsec)# pre-shared-key v$bx8*c
```

ネットワーク リストの定義

最初に、組織の中央にある特定のネットワークへのセキュアなトラフィック フローを許可するネットワーク リストを定義します。次の項で使用する例では、ネットワーク アドレスは 172.16.1.0 255.255.255.0 および 192.168.1.0 255.255.255.0 で、ネットワーク リストの ID は split です。

CLI コマンドを使用した手順

ネットワーク リストを定義するには、access-list コマンドを使用します。この例で使用するコマンドのシンタックスは、次のとおりです。

access-list *identifier* **standard permit** *ipaddress*

（注）　アクセス リストは標準タイプでも拡張タイプでもかまいません。

これらのアドレスへのトラフィックを許可するには、次の **access-list** コマンドを使用します。

```
hostname(config)# access-list split standard permit 172.16.1.0 255.255.255.0
hostname(config)# access-list split standard permit 192.168.1.0 255.255.255.0
```

ASDM を使用した手順

この項では、ASDM を使用してスプリット トンネリング用のネットワーク リストを設定する方法について説明します。ASDM の Group Policy パネルで、グループ ポリシーに名前を付け、ネットワーク リストおよびその他のスプリット トンネリング パラメータを定義します。

ネットワーク リストを定義するには、Group Policy Add/Edit Client Configuration タブからアクセスできる **ACL Manager** を使用します。スプリット トンネリング用のネットワーク リストを追加します（または既存のグループを編集します）。

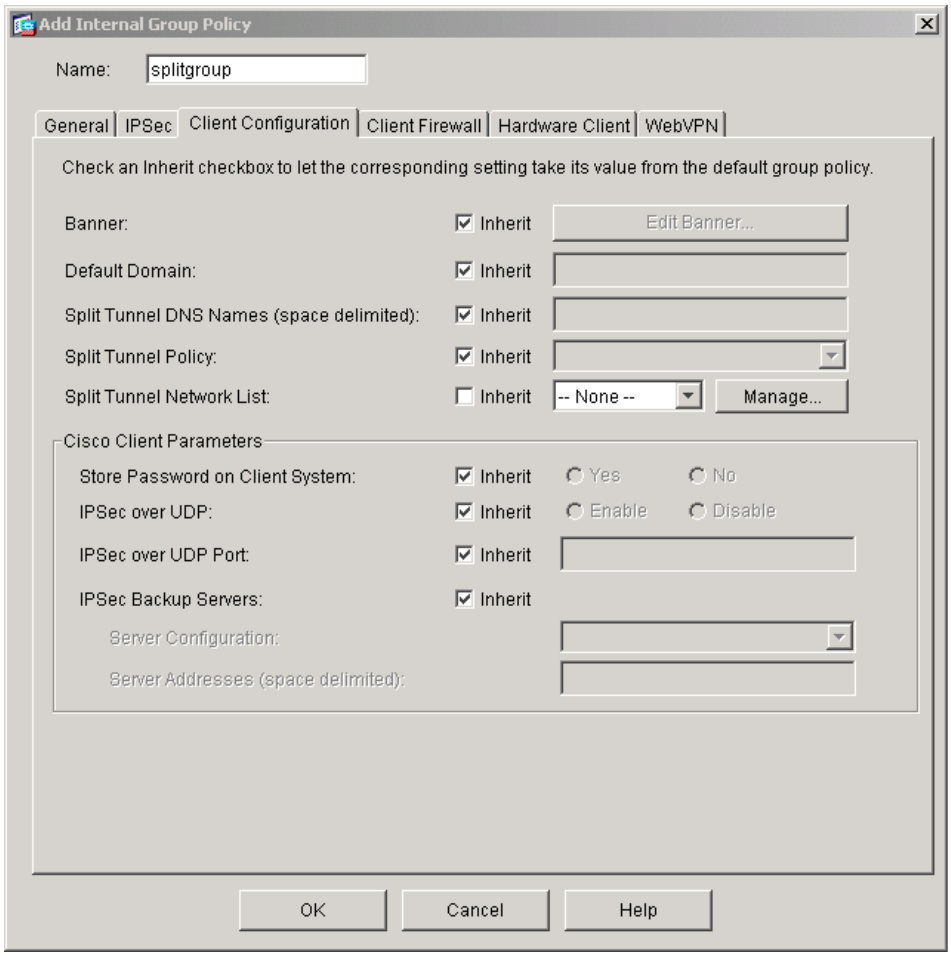
ステップ 1　Configuration > VPN > General > Group Policy パネルで **Add** をクリックし、メニューから **Internal Group Policy** を選択します。Add Internal Group Policy ダイアログボックスが表示され、General タブが示されます。

RADIUS などの外部サーバを選択するには、**External** オプションをクリックして、サーバ情報を入力します。

ステップ 2　新しいグループの名前を Name フィールドに入力します。この例では、名前は splitgroup です。

ステップ 3　**Client Configuration** タブをクリックします。Client Configuration オプションが表示されます（図 5-1 を参照してください）。

図 5-1　Add Internal Group Policy ダイアログボックス：Client Configuration



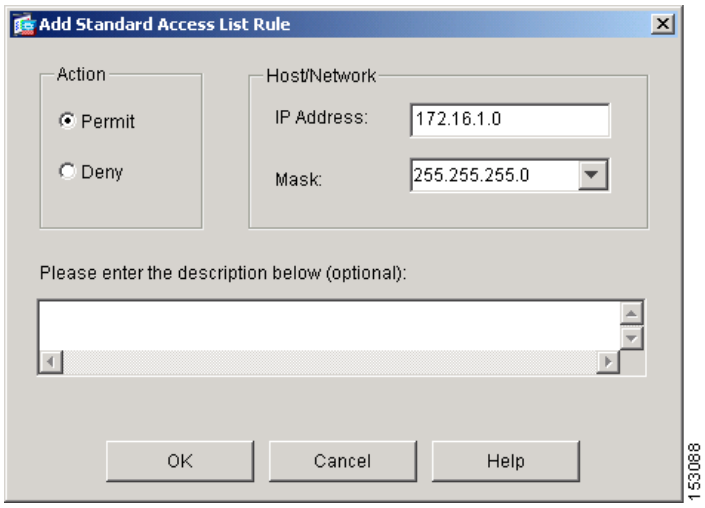
ステップ 4　ネットワーク リストの定義を開始するには、Split Tunnel Network List の横にある **Inherit** チェックボックスをオフにします。

ステップ 5　**Manage** をクリックします。ACL Manager テーブルが表示されます。

ステップ 6　ACL を追加するには、**Add** をクリックします。**ACL ID** フィールドに ACL の ID を入力し、**OK** をクリックします。この例では、名前は split です。

ステップ 7　**Add ACE** をクリックします。Add Standard Access List Rule ダイアログボックスが表示されます（図 5-2 を参照してください）。

図 5-2　スプリット トンネリング用の ACL の追加



ステップ 8　オプションを次のように設定します。

- Action オプション：ネットワーク リストに当該ネットワークを含めるには、**Permit** オプションをクリックします。
- Host/Network 領域：企業ネットワークまでトラフィックをセキュアにトンネリングできるように、含める各ホストまたはネットワークの IP アドレスとサブネット マスクを設定します。
  - IP Address：テキスト フィールドに IP アドレスを入力します。この例では、IP アドレスは 172.16.1.0 です。
  - Mask：リストでサブネット マスクをクリックします。この例では、サブネット マスクは 255.255.255.0 です。

ステップ 9　**OK** をクリックし、新しいグループ ポリシーのために Add Group Policy ダイアログボックスに戻ります。

スプリット トンネリング グループ ポリシーの作成

次の項では、スプリット トンネリング グループ ポリシーを作成する方法、またはデフォルトのグループ ポリシー（DfltGrpPolicy）を変更する方法について説明します。この例のコンフィギュレーション手順では、splitgroup という名前の、スプリット トンネリング用の特定の内部グループ ポリシーを作成します。

CLI コマンドを使用した手順

group-policy コマンドを使用して、config-group-policy モードでスプリット トンネリング ポリシーを設定します。split-tunnel-policy アトリビュートには次のオプションがあります。

- excludespecified：指定したネットワークのみ除外します。ネットワーク リスト内のアドレス宛のデータを除くすべてのデータを、セキュアな IPSec トンネルを介して送信します。この場合は、指定したネットワークまたはホスト宛のトラフィックを除くすべてのトラフィックが ASA のトンネルを通過します。

- tunnelall：すべてをトンネリングします。これがデフォルトのスプリット　トンネリング　ポリシーで、スプリット トンネリングはディセーブルになります。これが設定されている場合、トンネル グループ内のリモート クライアントからのトラフィックはすべて、暗号化された形式でセキュアな IPSec トンネルを通過します。
- tunnelspecified：指定したネットワークのみトンネリングします。セキュアな IPSec トンネルを介して、ネットワーク リスト内のアドレスにデータを送信します。その他のアドレス宛てのデータは、クリア テキストで伝送されます。このオプションを指定すると、リモート ユーザは、企業ネットワークを通じてトンネリングされることなくインターネット ネットワークにアクセスできると同時に、セキュアなトンネルを介して企業ネットワーク上の指定のリソースを使用できます。

次のコマンド例では、**tunnelspecified** オプションを使用して、ステップ 1 で作成したネットワーク リストに含まれるネットワークまでトラフィックをトンネリングします。

```
hostname(config)# group-policy splitgroup internal
hostname(config)# group-policy splitgroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value split
```

ASDM を使用した手順

スプリット トンネリング用に既存のグループ ポリシーを編集することも、新しいグループ ポリシーを追加することもできます。スプリット トンネリング用に既存のグループ ポリシーを編集する場合、次の手順を実行します。

ステップ 1　以前に作成したグループの Add Group Policy ダイアログボックスで **Client Configuration** タブを選択します（図 5-1 を参照してください）。この例では、以前に作成したグループ ポリシーは splitgroup です。

ステップ 2　Split Tunnel Policy の横にある **Inherit** チェックボックスをオフにし、次のいずれかをクリックします。

- Tunnel All Networks：デフォルトのスプリット トンネリング ポリシーです。スプリット トンネリングはディセーブルになります。これが設定されている場合、トンネル グループ内のリモート クライアントからのトラフィックはすべて、暗号化された形式でセキュアな IPSec トンネルを通過します。トラフィックがクリア テキストで伝送されたり、ASA 以外の宛先に伝送されたりすることはありません。トンネル グループ内のリモート ユーザは、ローカル ネットワークにはアクセスせず、企業ネットワークを経由してインターネット ネットワークに到達します。
- Tunnel Network List Below：セキュアな IPSec トンネルを介して、ネットワーク リスト内のアドレスにデータを送信します。その他のアドレス宛てのデータは、クリア テキストで伝送されます。このオプションを指定すると、リモート ユーザは、企業ネットワークを通じてトンネリングされることなくインターネット ネットワークにアクセスできると同時に、セキュアなトンネルを介して企業ネットワーク上の指定のリソースを使用できます。
- Exclude Network List Below：ネットワーク リスト内のアドレス宛のデータを除くすべてのデータを、セキュアな IPSec トンネルを介して送信します。この場合は、指定したネットワークまたはホスト宛のトラフィックを除くすべてのトラフィックが ASA のトンネルを通過します。

  Exclude Network List Below オプションを使用すると、トンネル グループ内のすべてのユーザが、ローカル ネットワーク上のすべてのデバイスにアクセスできます。ユーザによるアクセスをローカル ネットワーク上の指定のデバイスに制限するには、トンネル グループ内のリモート ユーザがアクセスするローカル デバイスのアドレスを知っている必要があります。これらのアドレスからネットワーク リストを作成し、Split Tunneling Network List からネットワーク リストを選択します。1 つのトンネル グループには 1 つのネットワーク リストしか適用できません

が、1 つのネットワーク リストには最大 10 個のネットワーク エントリを含めることができます。Cisco VPN クライアントで **Local LAN Access** をイネーブルにする必要もあります。詳細については、『*Cisco VPN Client Administrator Guide*』を参照してください。

この例では、**Tunnel Network List Below** をクリックします。

ステップ 3　Split Tunnel Network List の横にある **Inherit** チェックボックスをオフにし、メニューから ACL を選択します。この例では **split** を選択します。

ステップ 4　**OK** をクリックし、Configuration > VPN > General > Group Policy パネルに戻ります。

ステップ 5　**Apply** をクリックし、新しい ACL とグループ ポリシーを実行コンフィギュレーションに追加します。

スプリット トンネリング用のトンネル グループの設定

最後に、次のいずれかの項の手順を使用して、スプリット トンネリング用のトンネル グループを追加するか、既存のグループを編集します。この手順の例では、splittunnel という名前のリモート アクセス トンネル グループを追加し、そのグループに、スプリット トンネリングを提供するデフォルトのグループ ポリシーを割り当てる方法を示しています。

CLI コマンドを使用した手順

スプリット トンネリング用のトンネリング グループを作成する手順は、次のとおりです。

```
hostname(config)# tunnel-group splittunnel type ipsec_ra
hostname(config)# tunnel-group splittunnel general-attributes
hostname(config-general)# default-group-policy splitgroup
hostname(config)# tunnel-group splittunnel ipsec-attributes
hostname(config-ipsec)# pre-shared-key v$bx8*c
```

ASDM を使用した手順

スプリット トンネリング用のトンネリング グループを作成する手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Tunnel Group パネルで **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 **IPSec for Remote Access** を選択します。

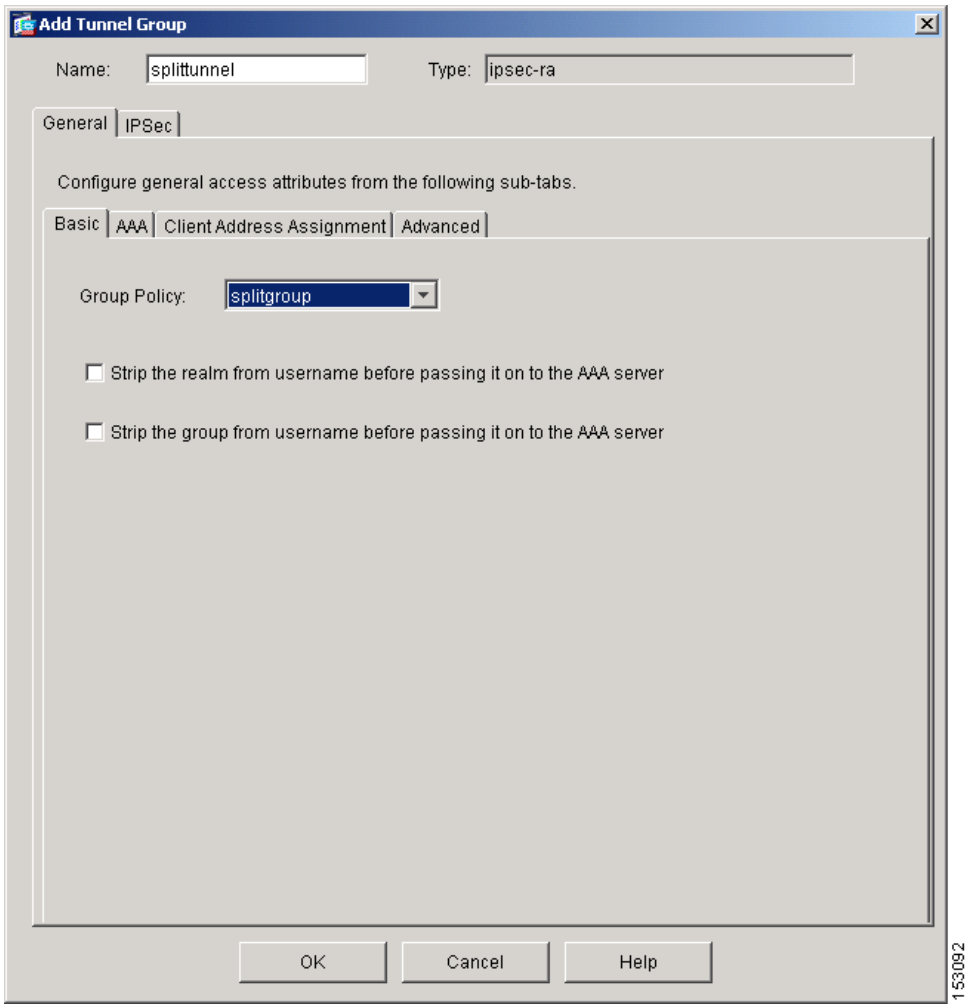
Add Tunnel Group ダイアログボックスが表示されます。

ステップ 2　**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、名前は splittunnel です。

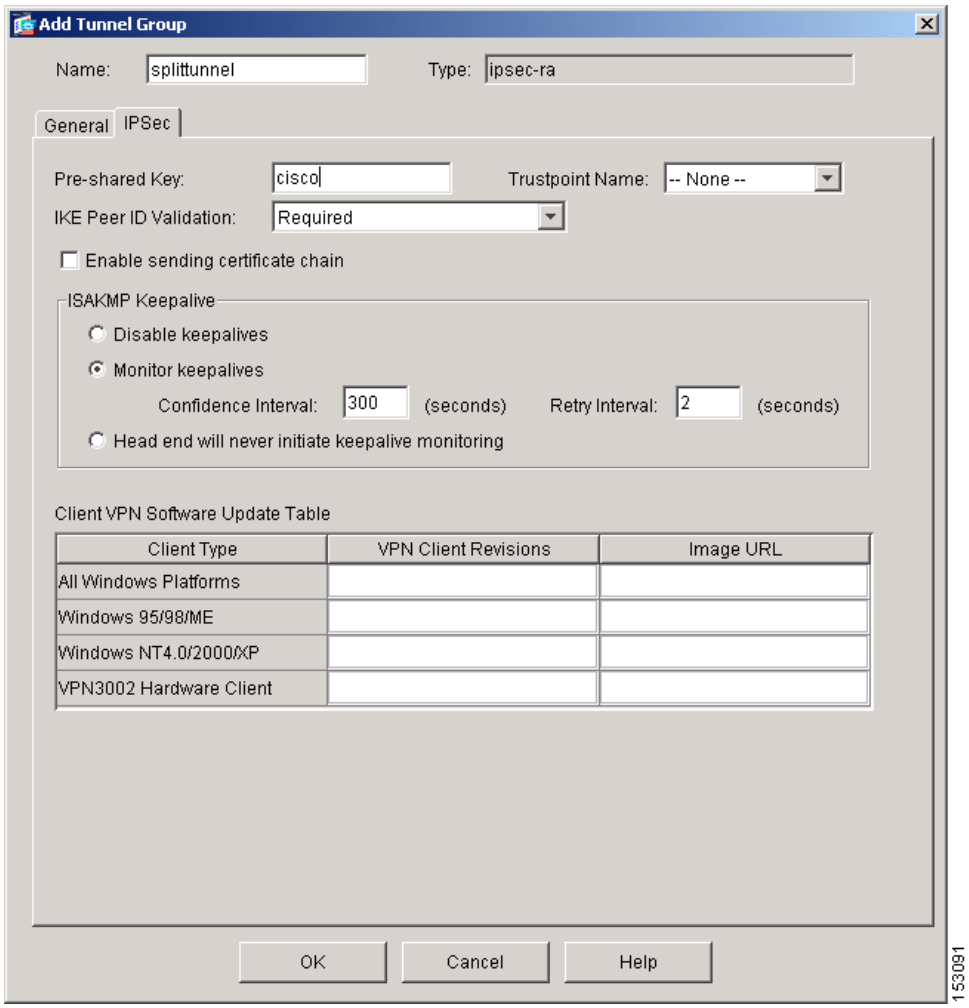
ステップ 3　**General** タブ、**Basic** タブの順にクリックし、次に Group Policy リストからグループ ポリシーを選択します。この例では、前の項で設定したグループ ポリシーである **splitgroup** をクリックします（図 5-3 を参照してください）。

図 5-3　Tunnel Group の追加：General タブと Basic タブ



ステップ 4　**IPSec** タブをクリックし、**Pre-shared Key** フィールドに事前共有鍵を入力します。この例では、**cisco** と入力して **OK** をクリックします。次に **Apply** をクリックします（図 5-4 を参照してください）。

図 5-4　トンネル グループの追加：IPSec タブ



ステップ 5　**OK** をクリックし、Configuration > VPN > General > Tunnel Group パネルに戻ります。

ステップ 6　**Apply** をクリックし、新しいトンネル グループをセキュリティ 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。

スプリット DNS 名

スプリット DNS を使用すると、集中定義された*ローカル ドメイン名*を内部 DNS サーバで解決できるようになります。それ以外のすべての DNS 要求は、ISP で割り当てられた DNS サーバによって解決されます。これは、スプリット トンネリング接続用です。トンネルを通過するトラフィックのドメイン名は内部 DNS サーバにより解決され、クリア テキストでインターネットに伝送される DNS 要求は、ISP で割り当てられた DNS サーバにより解決されます。

ASA では、Microsoft VPN クライアントのスプリット DNS はサポートされていません。ただし、Microsoft Windows オペレーティング システムで動作する Cisco VPN クライアントのスプリット DNS はサポートされています。

内部サーバにより解決される各ドメイン名を入力します。名前を区切るために使用できるのはスペースだけです。

クライアント ファイアウォールおよび VPN の設定

（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 クライアントだけで使用可能です。現在、ハードウェア クライアントまたはその他の（Windows 以外の）ソフトウェア クライアントでは使用できません。

トンネル グループ内のリモート ユーザがスプリット トンネリングを設定すると、クライアント ファイアウォールのセキュリティは強化されます。この場合、ファイアウォールは、インターネットまたはユーザのローカル LAN を経由した侵入からユーザの PC を保護することにより、企業ネットワークを保護します。

VPN クライアントから ASA に接続しているリモート ユーザは、2 つのファイアウォール オプションのいずれかを選択できます。

1 つ目のオプションは、リモート ユーザの PC にパーソナル ファイアウォールをインストールすることです。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たファイアウォール ポリシーを強制的に適用し、動作を確認するためにファイアウォールを監視します。ファイアウォールの動作が停止すると、VPN クライアントは ASA 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は *Are You There（AYT）*と呼ばれます。これは、VPN クライアントが「are you there?」というメッセージを定期的に送信することによってファイアウォールを監視するためです。応答がない場合、VPN クライアントはファイアウォールがダウンしていると判断し、セキュリティ アプライアンスへの接続を終了します）。ネットワーク管理者が元々これらの PC ファイアウォールを設定している場合がありますが、この方法を使用すれば、ユーザは独自のコンフィギュレーションをカスタマイズできます。

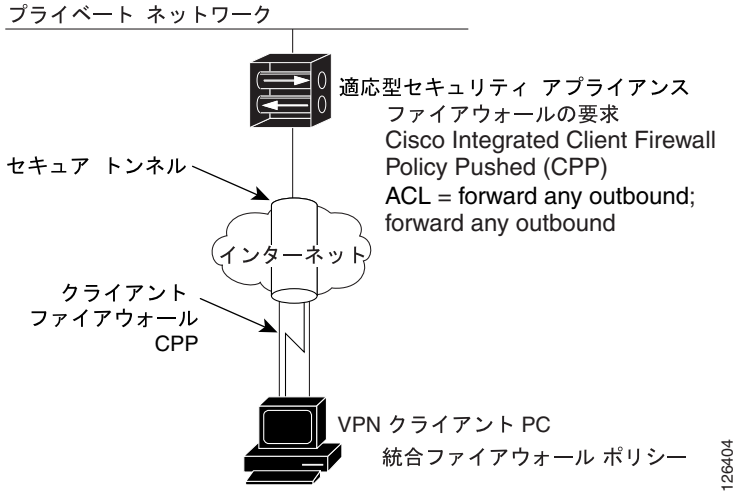
2 つ目のオプションは、パーソナル ファイアウォール用の集中型ファイアウォール ポリシーを VPN クライアント PC に強制的に適用することです。スプリット トンネリングを使用して、トンネル グループ内のリモート PC に対するインターネット トラフィックをブロックすることは、この方法の一般的な例です。この方法では、トンネルが確立されている間、インターネット経由の侵入から PC を保護することにより、中央のサイトを保護します。このファイアウォール シナリオは、*プッシュ ポリシー*または *Central Protection Policy（CPP）*と呼ばれます。ASA で、VPN クライアントに強制的に適用するファイアウォール ポリシーとして CPP を指定し、着信トラフィックおよび発信トラフィック用の ACL を追加します。ASA によってこのポリシーが VPN クライアントにプッシュされます。ポリシーは VPN クライアントによりローカルの Cisco Integrated Client ファイアウォールに渡され、そこで強制適用されます。

デフォルトとして使用するクライアント ファイアウォールの設定

この項の手順では、例として次のシナリオを使用します（図 5-5 を参照してください）。

- ファイアウォールが必要。ファイアウォール タイプは、Cisco Integrated Client Firewall です。
- スプリット トンネリング コンフィギュレーションでデフォルトとして使用できるアクセス リストが 2 つある。1 つ目のアクセス リストは、インターネット（またはトンネルの外側にある他のサイト）から VPN クライアントに着信する非請求トラフィックをすべて拒否します。この ACL は FWBlockIn と呼ばれます。2 つ目のアクセス リストは、VPN クライアントからトンネルの外側にあるサイトへの発信トラフィックを許可します。この ACL は FWAllowAnyOut と呼ばれます。プロトコルはどちらも IP です。

図 5-5　スプリット トンネリング コンフィギュレーション用に Cisco Integrated Client Firewall を使用したシナリオ



クライアント ファイアウォール コンフィギュレーション用のアクセス リストの設定（CLI）

この例で使用するクライアント アクセス リストを設定する CLI コマンドは、次のとおりです。

```
hostname(config)# access-list FWBlockIn deny ip any any
hostname(config)# access-list FWAllowAnyOut permit ip any any
hostname(config)# group-policy GroupPolicy4 attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWBlockIn
acl-out FWAllowAnyOut
```

1 つ目の **access-list** コマンドは、VPN クライアントへのすべての着信トラフィックをブロックするためのデフォルトとして動作できます。ACL の ID は FWBlockIn です。アクションは deny、プロトコルは ip です。送信元のアドレス / マスク、および宛先のアドレス / マスクは、両方とも any です（任意の場所から VPN クライアントへのトラフィックをすべてブロックします）。

2 つ目のコマンドは、VPN クライアントまたは VPN クライアントのグループからの発信トラフィックをすべて許可します。この ACL の ID は FWAllowAnyOut です。アクションは permit、プロトコルは ip です。送信元のアドレス / マスク、および宛先のアドレス / マスクは、両方とも any です（送信元から宛先へのトラフィックをすべて許可します）。

グループ ポリシーでのクライアント ファイアウォールの設定

この項では、CLI および ASDM で、グループ ポリシーの一部としてクライアント ファイアウォールを設定するための手順を示します。

CLI コマンドを使用した手順

show running-config group-policy *name* コマンドを使用すると、特定のグループ ポリシーの実行コンフィギュレーションを表示できます。

リモート ユーザ用の VPN クライアントまたは VPN クライアントのグループのファイアウォールを設定するには、**group-policy** コマンドを使用します。この例で使用するコマンドのシンタックスは、次のとおりです。

group-policy *name* **attributes**

client-firewall opt | **req cisco-integrated acl-in** *ACL* **acl-out** *ACL*

次のコマンドは、GroupPolicy4 という名前のグループ ポリシーを作成し、config-group-policy モードに移行して Cisco Integrated Firewall を要求するクライアント ファイアウォールを設定します。着信 ACL は FWBlockIn で、発信 ACL は FWAllowAnyOut です。この例を使用すると、デフォルト ファイアウォール ポリシーの設定を完了できます。

```
hostname(config)# group-policy GroupPolicy4 attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWBlockIn
acl-out FWAllowAnyOut
```

ASDM を使用した手順

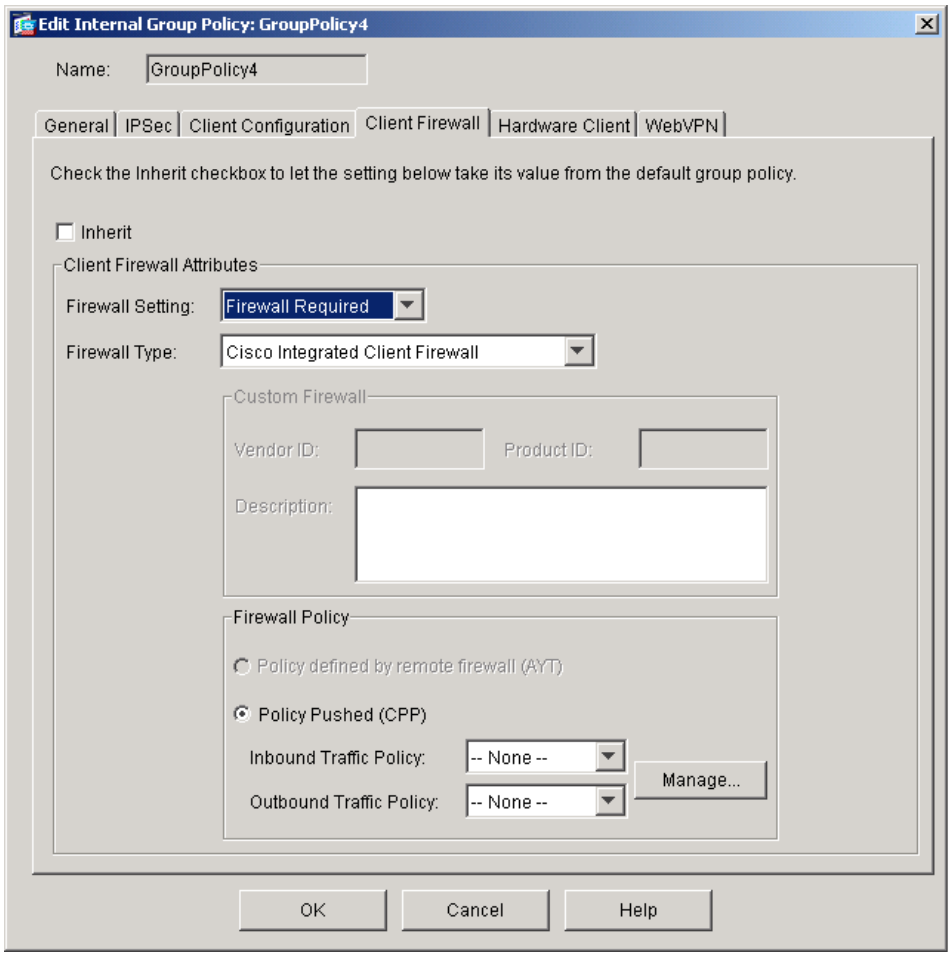
ASDM を使用してクライアント ファイアウォール プロテクションを設定するには、グループ ポリシーを追加するか、既存のグループ ポリシーを編集します。この例では、GroupPolicy4 という名前の既存のポリシーを編集します。

ステップ 1　Configuration > VPN > General > Group Policy パネルで、テーブルからグループ ポリシーを選択し、**Edit** をクリックします。ASDM に Edit Group Policy ダイアログボックスが表示されます。

ステップ 2　**Client Firewall** タブをクリックします。図 5-6 は、この例で設定されているクライアント ファイアウォール オプションを示しています。

- Inherit：オフ（ディセーブル）
- Firewall Setting：Firewall Required
- Firewall Type：Cisco Integrated Client Firewall
- Firewall Policy：Policy Pushed (CPP)

図 5-6　クライアント ファイアウォール オプション



ステップ 3　**Inherit** チェックボックスをオフにします。

ステップ 4　ファイアウォール設定を選択するには、Firewall Setting リストで対象のオプションをクリックします。この例では、Firewall Required を設定します。このリストには、次のオプションが含まれています。

- No Firewall : このトンネル グループ内のリモート ユーザにはファイアウォールが必要ありません。これがデフォルト設定です。
- Firewall Required : このトンネル グループ内のすべてのリモート ユーザは、特定のファイアウォールを使用する必要があります。指定のファイアウォールを使用しているユーザだけが接続できます。

  この例と同じように Firewall Required を選択した場合、トンネル グループ内のすべてのユーザは、指定されたファイアウォールを使用する必要があります。サポートされている指定のファイアウォールがインストールされ動作していない場合、接続を試行するすべてのセッションは ASA によりドロップされます。この場合は、ファイアウォール コンフィギュレーションが一致しないことを ASA が VPN クライアントに通知します。

（注）　トンネル グループ用のファイアウォールが必要な場合は、当該トンネル グループに Windows ベースの VPN クライアント以外のクライアントが含まれていないことを確認してください。トンネル グループに他のクライアントが含まれている場合（ハードウェア クライアントを含む）、それらのクライアントからは接続できません。

- Firewall Optional：このトンネル グループ内のすべてのリモート ユーザが接続できます。指定されたファイアウォールがある場合、ユーザはそれを使用できます。ファイアウォールがないユーザは、警告メッセージを受信します。

  トンネル グループ内のリモート ユーザがファイアウォール機能を使用できない場合は、Firewall Optional をクリックします。Firewall Optional 設定を使用すると、トンネル グループ内のすべてのユーザが接続できます。ファイアウォールがあるユーザは、それを使用できます。ファイアウォールがない状態で接続するユーザは、警告メッセージを受信します。

  この設定は、ファイアウォールがサポートされているユーザとファイアウォールがサポートされていないユーザが混在するトンネル グループを作成する場合に役立ちます。たとえば、トンネル グループを変更しつつあり、グループ内に、ファイアウォール機能の設定が完了したメンバと、ファイアウォールが設定されていないメンバが両方含まれる場合などです。

ステップ 5　Firewall Type リストからファイアウォールを選択します。この例では、Cisco Integrated Client Firewall を指定します。

指定するファイアウォールは使用できるファイアウォール ポリシーと相関関係にあるので注意してください。設定するファイアウォールによって、サポートされるファイアウォール ポリシー オプションが決まります（詳細については 表 5-1 を参照してください）。

次のいずれかをクリックします。

- **Cisco Integrated Client Firewall**：Cisco VPN クライアントに組み込まれているステートフル ファイアウォール。
- **Cisco Security Agent**：Cisco 侵入防御（サーバおよびデスクトップ システムに対する脅威からの保護）。
- **Custom Firewall**：同じベンダーからのファイアウォールの組み合せ、またはリストに含まれていない他のファイアウォール。このオプションを選択した場合、**Custom Firewall** グループ ボックスで独自のファイアウォールのリストを作成する必要があります。カスタム ファイアウォールを設定する手順は、このマニュアルには含まれていません。
- **Network ICE BlackICE Defender**：Network ICE BlackICE Agent または Defender パーソナル ファイアウォール。
- **Sygate Personal Firewall**
- **Sygate Personal Firewall Pro**
- **Sygate Security Agent**：Sygate Security Agent パーソナル ファイアウォール。
- **Zone Labs ZoneAlarm**：Zone Labs ZoneAlarm パーソナル ファイアウォール。
- **Zone Labs ZoneAlarm or ZoneAlarm Pro**：Zone Labs ZoneAlarm パーソナル ファイアウォールまたは Zone Labs ZoneAlarm Pro パーソナル ファイアウォールのいずれか。
- **Zone Labs ZoneAlarm Pro**：Zone Labs ZoneAlarm Pro パーソナル ファイアウォール。

ステップ 6　ファイアウォール ポリシーを選択するには、Firewall Policy グループ ボックスで対象のオプションをクリックします。

設定したファイアウォールに応じて、特定のファイアウォール ポリシー オプションを使用できます（表 5-1 を参照してください）。

表 5-1　各ファイアウォールで使用できるファイアウォール ポリシー オプション

ファイアウォール	Policy Defined by Remote Firewall (AYT)	Policy Pushed (CPP)
Cisco Integrated Client Firewall	使用不可	使用可
Cisco Security Agent	使用可	使用不可
Network ICE BlackICE Defender	使用可	使用不可
Sygate Personal Firewall	使用可	使用不可
Sygate Personal Firewall Pro	使用可	使用不可
Sygate Security Agent	使用可	使用不可
Zone Labs ZoneAlarm	使用可	使用可
Zone Labs ZoneAlarm or Zone Labs ZoneAlarm Pro	使用可	使用可
Zone Labs ZoneAlarm Pro	使用可	使用可

ステップ 7　ファイアウォール ポリシーに関連付けられているオプションから選択します。

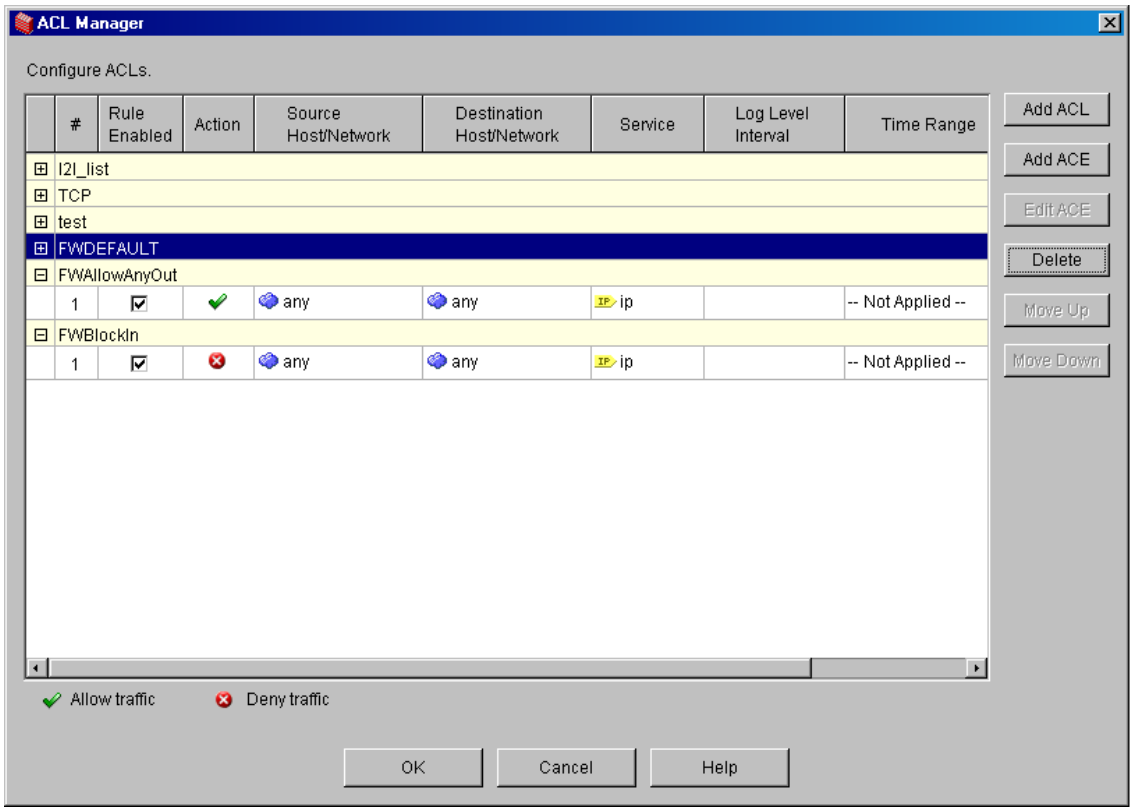
この例では、Policy Pushed (CPP) を指定します。Firewall Policy リストには、次のオプションが含まれています。

- Policy defined by remote firewall (AYT) : このトンネル グループ内のリモート ユーザの PC には、ファイアウォールが配置されています。ローカル ファイアウォールは、VPN クライアントにファイアウォール ポリシーを強制的に適用します。ASA は、指定のファイアウォールが VPN クライアントにインストール済みで動作している場合のみ、VPN クライアントの接続を許可します。指定のファイアウォールが実行されていない場合、接続は失敗します。接続が確立されると、VPN クライアントは、30 秒ごとにファイアウォールにポーリングすることにより、ファイアウォールが動作中であることを確認します。ファイアウォールの動作が停止すると、VPN クライアントはセッションを終了します。
- Policy Pushed (CPP)：ASA は、次の Policy Pushed（CPP）リストでユーザが選択した ACL で定義されているトラフィック管理規則を、VPN クライアントに強制的に適用します。
  - Inbound Traffic Policy：VPN クライアントへの着信トラフィックを制御するための ACL を選択します。
  - Outbound Traffic Policy : VPN クライアントからの発信トラフィックを制御するための ACL を選択します。

  VPN クライアントにローカル ファイアウォールも配置されている場合、ASA からプッシュされたポリシーは、ローカル ファイアウォールのポリシーと共存します。*いずれか*のファイアウォールの規則によりブロックされたパケットは、ドロップされます。

ステップ 8　CPP を選択した場合、Inbound Traffic Policy リストおよび Outbound Traffic Policy リストで、ACL をクリックします。ASDM では、両方のリストで同じ ACL を選択することはできません。リストに ACL を追加するには、**Manage** をクリックします。ACL Manager テーブルが表示されます。この例では、2 つの ACL を追加します。1 つは着信トラフィック ポリシーとして、もう 1 つは発信トラフィック ポリシーとして使用します（図 5-7 を参照してください）。

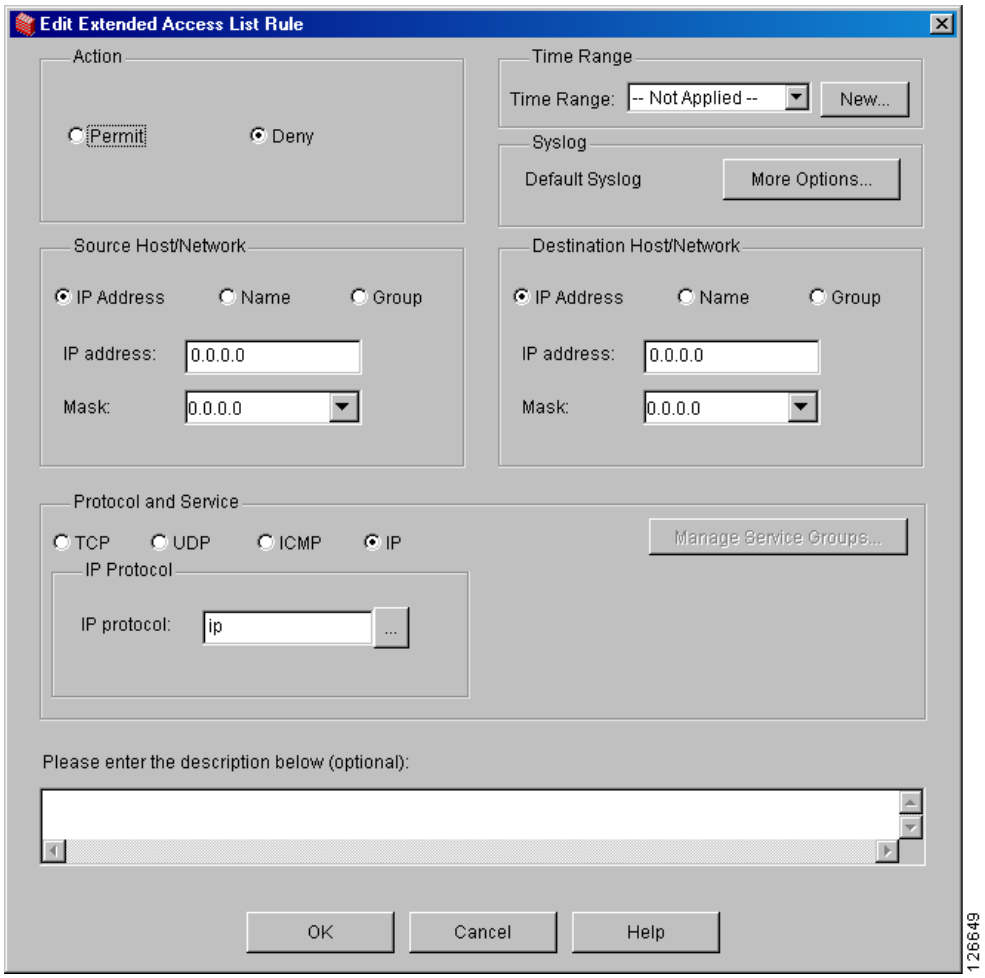
図 5-7　ACL Manager の使用



ステップ 9　ACL を追加するには、**Add ACL** をクリックし、ACL の名前を ACL ID ボックスに入力して **OK** をクリックします。着信 ACL の場合、名前は ID としての FWBlockIn です。

ステップ 10　前のステップで追加した **FWBlockIn** ACL をクリックし、次に **Add ACE** をクリックしてアクセス コントロール エントリを挿入します。Add Extended Access List Rule ダイアログボックスが表示されます。すべてのフィールドの詳細を参照する場合は、**Help** をクリックします（図 5-8 を参照してください）。

図 5-8　アクセス リスト規則の追加



a. CPP ポリシーの場合、非請求ネットワークおよびホストから VPN クライアントまたは VPN クライアントのグループへのすべてのトラフィックを拒否する必要があります。そのように設定するには、**Deny** オプションをクリックします。Source Host/Network および Destination Host/Network で、デフォルトの **0.0.0.0**（任意）を受け入れます。

b. IP をデフォルトのプロトコルとして設定するには、Protocol and Service グループ ボックスで **IP** オプションをクリックします。送信元と宛先の両方で、デフォルトのサービスは any です。これらを変更する場合の詳細については、**Help** をクリックしてください。

c. **OK** をクリックして ACE を追加します。

ステップ 11　同じ手順を実行して、VPN クライアントからのすべての発信トラフィックを許可する 2 つ目の ACL を追加します。

a. ACL ID ボックスに *FWAllowAnyOut* と入力します。

b. **Add ACE** をクリックします。Add/Edit Extended Access List Rule ダイアログボックスが表示されたら、Action では **Permit** をクリックし、Protocol では **IP** をクリックします。

ステップ 12　**OK** をクリックします。ASDM に ACL Manager が表示されるので、ACL が追加されたことを確認します。図 5-7 を参照してください。

ステップ 13　**OK** をもう一度クリックします。ASDM に Client Firewall タブが表示されます。

ステップ 14　Policy Pushed (CPP) オプションで、着信トラフィック ポリシーおよび発信トラフィック ポリシーを設定します。

a.　Inbound Traffic Policy リストで **FWBlockIn** をクリックします。

b.　Outbound Traffic Policy リストで **FWAllowAnyOut** をクリックします。

c.　**OK** をクリックします。ASDM に Group Policy パネルが表示されます。

ステップ 15　**Apply** をクリックしてから、設定を保存します。

HTTP トラフィックを許可するためのクライアント ファイアウォールの設定

HTTP トラフィックの着信を許可し、他の着信トラフィックをすべてブロックするようにクライアント ファイアウォールを設定できます。この例では、発信トラフィック ポリシーとして、前の項で作成した FWAllowAnyOut を使用します。

CLI コマンドを使用した手順

HTTP トラフィックを許可し、他のすべての着信トラフィックを拒否するには、次の **access-list** コマンドをコンフィギュレーション モードで実行します。ACL の名前は FWAllowHTTP、使用するプロトコルは TCP、HTTP トラフィックのポート番号は 80 です。

ステップ 1　ACL を設定します。最初の 2 つのコマンドは着信トラフィック ポリシーを定義し、3 つ目のコマンドは発信トラフィック ポリシーを定義します。

```
hostname(config)# access-list FWAllowHTTP permit tcp any any eq 80
hostname(config)# access-list FWAllowHTTP deny ip any any
hostname(config)# access-list FWAllowAnyOut permit ip any any
```

ステップ 2　group-policy モードで client-firewall コマンドを入力します。この例では、グループ ポリシーの名前は ClientServer です。

```
hostname(config)# group-policy ClientServer internal
hostname(config)# group-policy ClientServer attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWAllowHTTP
acl-out FWAllowAnyOut
```

ASDM を使用した手順

ASDM を使用して Cisco Integrated Client Firewall および CPP を設定する手順は、次のとおりです。

（注）　詳細については、「グループ ポリシーでのクライアント ファイアウォールの設定」を参照してください。

ステップ 1　Configuration > VPN > General > Group Policy で、グループ ポリシーを追加または編集します。この例では、新しいポリシーを追加します。

ステップ 2　**Add** をクリックし、**Internal Group Policy** を選択します。

ステップ 3　新しいポリシーの名前を Name フィールドに入力します。この例では、ClientServer という名前のポリシーを追加します。

ステップ 4　**Client Firewall** タブをクリックします。

ステップ 5　**Inherit** オプションをクリックして、オフにします。

ステップ 6　Firewall Setting リストで、**Firewall Required** オプションをクリックします。

ステップ 7　Firewall Type として **Cisco Integrated Client Firewall** を保持します。

この設定では、Firewall Policy グループ ボックスの Policy Pushed (CPP) オプションが自動的にイネーブルになります。

ステップ 8　**Manage** をクリックします。

ステップ 9　**Add ACL** をクリックし、ACL ID ボックスに *FWAllowHTTP* という名前を入力して **OK** をクリックします。

ステップ 10　テーブル内の **FWAllowHTTP** をクリックし、**Add ACE** をクリックします。次のオプションを設定します。

a. Action で、デフォルトのオプション（**Permit**）を使用します。

b. デフォルトの Protocol and Service 設定（**TCP**）を使用します。このオプションを指定すると、その下の Service パラメータがイネーブルになります。

c. 左側でデフォルトの Service 演算子（=）を使用し、**...** をクリックします。表示されるリストで **www/http** をクリックし、**OK** をクリックします。

d. Destination Port の側で、デフォルト設定である **Service = any** を保持します。

e. **OK** をクリックします。

ステップ 11　**OK** をクリックします。

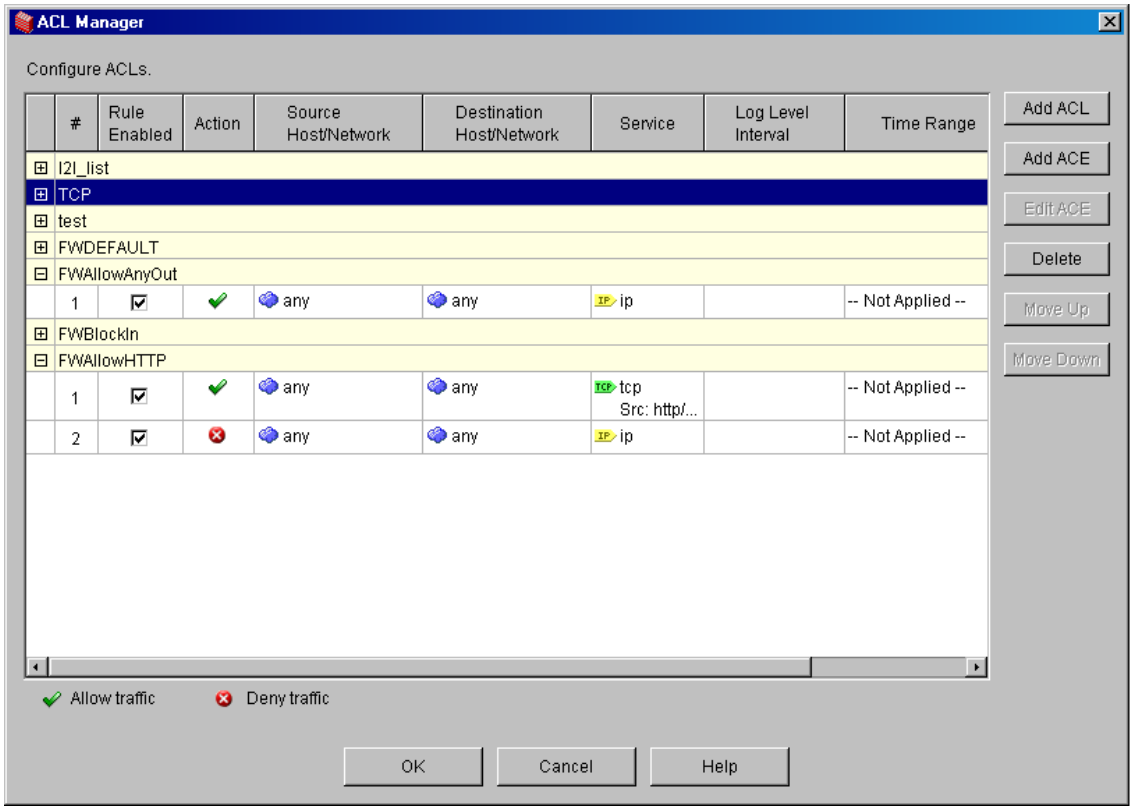
ステップ 12　Client Firewall タブの Firewall Policy および Policy Pushed (CPP) で、Inbound Traffic Policy リストに対して **FWAllowHTTP** をクリックし、Outbound Traffic Policy リストに対して **FWAllowAnyOut** をクリックします。次に **Manage** をクリックします。

ステップ 13　ACL Manager テーブル内の FWAllowHTTP ACL で **Add ACE** をクリックし、2 つ目の規則を追加します。

ここでは、すべてのトラフィックを拒否するように、別の規則を FWAllowHTTP に追加します（この規則は、HTTP トラフィックを許可する規則の後に追加されます）。

ステップ 14　Action で **Deny** を、Protocol and Service で **IP** をクリックし、次に **OK** をクリックします。図 5-9 は、この例での ACL Manager テーブルの最終的なコンフィギュレーションを示しています。FWAllowHTTP ACL に対し、2 つの規則が正しい順序で設定されていることに注意してください。HTTP から VPN クライアントへの着信トラフィックは通過できますが、その他のトラフィックはすべて拒否されます。

図 5-9　VPN クライアントを Web サーバとして使用するためのクライアント ファイアウォール ACL



ステップ 15　ACL Manager で **OK** をクリックします。

ステップ 16　Client Firewall タブで **OK** をもう一度クリックし、次に **Apply** をクリックします。

外部サーバを使用する認証

この例は、リモート アクセス ユーザの外部認証を設定する方法、具体的には RADIUS サーバを設定する方法を示しています。

コンフィギュレーション手順の概要

外部認証を設定するには、次の手順を実行します。

1. 認証用の AAA サーバ グループを作成します。
2. AAA サーバ グループにホストを追加します。
3. 外部認証用のリモート アクセス トンネル グループを追加または編集します。

この例では、次のシナリオを使用します。

- AAA サーバ グループの名前は ACSRadiusServer。
- AAA ホストの IP アドレスは、172.16.0.1、172.16.0.2、および 172.16.0.3。
- リモート アクセス トンネル グループの名前は、ACSRadiusGroup。

IP アドレス プールの作成

最初のステップは、コール インする VPN クライアント用の IP アドレス プールの作成です。別の方法として、DHCP サーバを使用して、IP アドレスをクライアントに配布することもできます。この例では、アドレス プールを使用します。

CLI コマンドを使用した手順

IP アドレス プールを作成するには、**ip local pool** コマンドを使用します。コマンドのシンタックスは、次のとおりです。

ip local pool *poolname first-address–last-address* [***mask*** *mask*]

たとえば、次のコマンドを入力して、名前が IPPool2 で、アドレス範囲が 10.20.30.40 から 10.20.30.60 の IP アドレス プールを作成します。

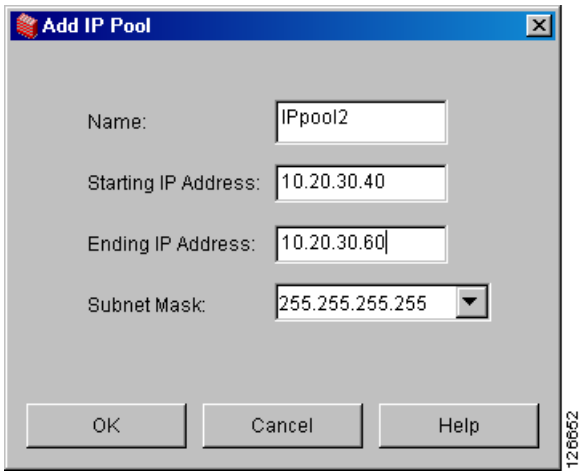
```
hostname(config)# ip local pool IPPool2 10.20.30.40-10.20.30.60
hostname(config)#
```

ASDM を使用した手順

IP アドレス プールを作成するには、次の手順を実行します。

ステップ 1　Configuration > VPN > IP Address Management > IP Pools で、**Add** をクリックします。ASDM に、Add IP Pool ダイアログボックスが表示されます（図 5-10 を参照してください）。

図 5-10　IP アドレス プールの追加



ステップ 2　**Name** フィールドに IP プールの名前を入力します。この例では、名前は IPpool2 です。

ステップ 3　**Starting IP Address** フィールドに開始 IP アドレスを入力します。この例では、開始 IP アドレスは 10.20.30.40 です。

ステップ 4　**Ending IP Address** フィールドに終了 IP アドレスを入力します。この例では、終了 IP アドレスは 10.20.30.60 です。

ステップ 5　**Subnet Mask** リストで、サブネット マスクをクリックします。ASDM では、サブネット マスクの設定は必須です。

ステップ 6　**OK** をクリックしてから、**Apply** をクリックします。

サーバ グループの追加

認証用に外部サーバ グループを追加します。この例では、次の機能を使用して、RADIUS 認証用に ACSRadiusServers という名前のサーバ グループを追加します。

- RADIUS プロトコル
- single アカウンティング モード
- timed リアクティベーション モード

  このオプションでは、サーバは、ダウン時間が 30 秒経過すると再度有効にされます。デフォルトの設定は、depletion です。この設定では、障害が発生したサーバは、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のみ再度有効にされます。
- サーバが無効になるまでに許容されている試行失敗の回数は 2

  デフォルト値は 3 です。

CLI コマンドを使用した手順

サーバ グループを設定するには、**aaa-server protocol** コマンドを使用します。このサーバ グループを RADIUS サーバ グループとして設定する **aaa-server protocol** コマンドのシンタックスは、次のとおりです。

aaa-server *server-tag* **protocol** *server-protocol*

aaa-server コマンドを入力すると、CLI は、AAA サーバ グループ アトリビュートを設定するための config-aaa-server-group モードに切り替わります。

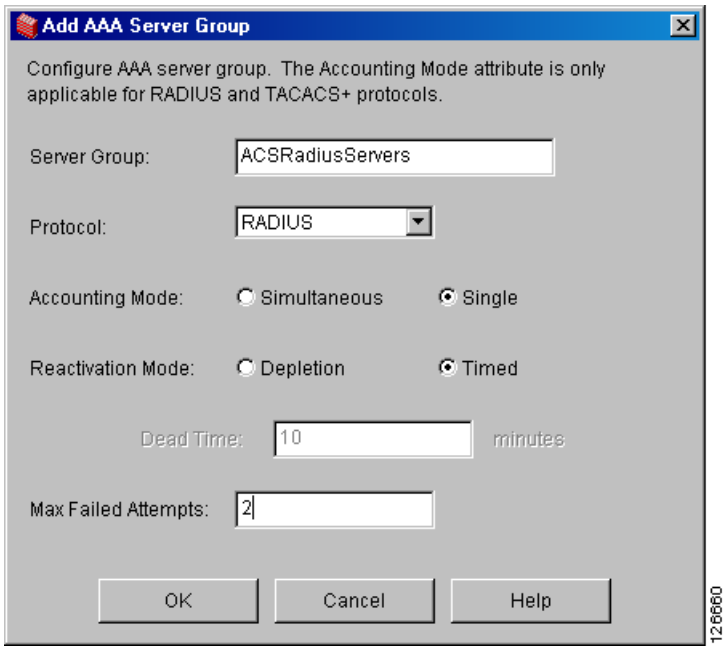
次のコマンドは、RADIUS プロトコルを使用する RadiusServer という名前の AAA サーバ グループを設定します。

```
hostname(config)# aaa-server ACSRadiusServers protocol radius
hostname(config-aaa-server-group)# accounting-mode single
hostname(config-aaa-server-group)# reactivation-mode timed
hostname(config-aaa-server-group)# max-failed-attempts 2
```

ASDM を使用した手順

ステップ 1　認証用のサーバ グループを設定するには、Configuration > Properties > AAA Setup > AAA Servers パネルの Server Groups 領域で **Add** をクリックします。ASDM に、Add AAA Server Group ダイアログボックスが表示されます（図 5-11 を参照してください）。

図 5-11　AAA サーバ グループの追加



ステップ 2　追加するサーバ グループの情報を入力します。

a. Server Group : このサーバ グループの名前を入力します。この例では、名前は ACSRadiusServers です。

Protocol : Protocol リストで、このサーバ グループで使用するプロトコルをクリックします。次のプロトコルから選択できます。この例では、プロトコルは RADIUS です。

- RADIUS
- TACACS+
- NT Domain
- SDI
- Kerberos
- LDAP
- HTTP Form

b. Accounting Mode : RADIUS または TACACS+ の場合、アカウンティング モード オプションとして **Simultaneous** または **Single**（デフォルト）をクリックします。simultaneous モードの ASA では、アカウンティング データがグループ内のすべてのサーバに送信されます。single モードの ASA では、アカウンティング データが 1 つのサーバにだけ送信されます。この例では、デフォルトの Single を受け入れます。

c. Reactivation Mode : 障害が発生したサーバを再度有効にする方法として Depletion または Timed を選択します。depletion モードでは、障害が発生したサーバは、グループ内のすべてのサーバが非アクティブになった後でのみ再度有効にされます。timed モードでは、障害が発生したサーバは、ダウン時間が 30 秒経過すると再度有効にされます。これらのオプションのいずれかをクリックします。デフォルトは Depletion です。この例では、timed リアクティベーション モードを使用します。

d. Dead Time : リアクティベーション モードが Depletion の場合、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イネーブルにするまでの経過時間を、分単位で設定する必要があります。デフォルトは 10 です。

e. Max Failed Attempts : 応答がないサーバをデッドと宣言するまでに許可されている接続試行失敗の回数。許可する試行回数を入力します。デフォルトは 3 です。この例では、値を 2 に設定します。

ステップ 3　**OK** をクリックしてから、**Apply** をクリックします。

AAA サーバ グループへの AAA ホストの追加

AAA サーバ グループを設定した後は、サーバ グループに追加している各ホストの IP アドレスを識別し、ホストが使用しているインターフェイスを識別することにより（オプション）、サーバ グループに AAA ホスト（この場合は RADIUS サーバ）を追加できます。

CLI コマンドを使用した手順

CLI のこの例では、内部インターフェイス上のサーバ グループ ACSRadiusServers に 3 個のホストを追加します。これらのコマンドは、ホスト IP アドレスを定義し、aaa-server-group モードで設定できるパラメータを示します。

aaa-server host コマンドのシンタックスは、次のとおりです。

aaa-server *server-tag* [(*interface-name*)] **host** *server-ip*

AAA サーバ ホストを追加するために使用する **aaa-server host** コマンドの例では、次のアトリビュートを参照します。

- **retry-interval**：接続を試行するまでに待機する秒数。デフォルト値は 10 です。
- **timeout**：ASA がプライマリ AAA サーバへの要求を断念し、バックアップ サーバ（存在する場合）にその要求を送信するまでの時間（分単位）。デフォルト値は 10 です。
- **key**：暗号鍵。大文字と小文字が区別されます。

```
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.1
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.2
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.3
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
```

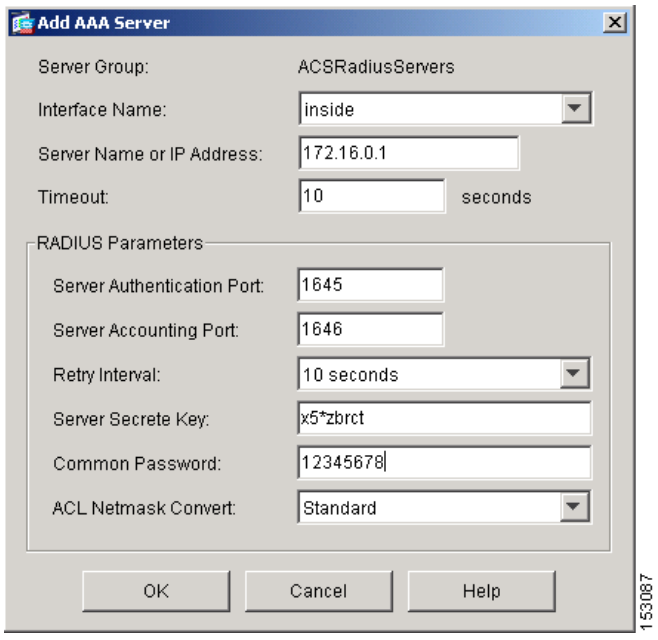
ASDM を使用した手順

ASDM を使用して、認証に RADIUS を使用する AAA サーバ グループに AAA サーバを追加する手順は、次のとおりです。

ステップ 1　Configuration > Properties > AAA Setup > AAA Servers パネルで、AAA サーバの追加先のサーバ グループをクリックします。この例では、**ACSRadiusServers** をクリックします。

ステップ 2　Servers の Selected Group 領域で **Add** をクリックします。ASDM に、Add AAA Server ダイアログボックスが表示されます。図 5-12 は、この例の値を設定するダイアログボックスを示しています。

図 5-12　外部認証用の AAA の追加



ステップ 3　グループ内の最初のホストについて、次の情報を入力します。

a. Interface Name：認証サーバに関連付けられたネットワーク インターフェイスの名前を、Interface Name リストから選択します。この例では、**inside** を選択します。

b. Server IP Address：AAA サーバの IP アドレスを入力します。この例では、追加する最初のホストの IP アドレスは 172.16.0.1 です。

c. Timeout：ASA がプライマリ AAA サーバへの要求を断念し、バックアップ サーバ（存在する場合）にその要求を送信するまでの時間を分単位で入力します。この例では、デフォルト設定の 10 秒を使用します。

d. RADIUS Parameters グループ：このグループ ボックスで各パラメータを設定します。この例では、配置場所のデフォルトを受け入れます。サーバの秘密鍵と共通のパスワードを入力する必要があります。

（注）　共通パスワードを使用するのは、RADIUS サーバだけです。

e. Server Authentication Port：ユーザ認証用のサーバ ポート。デフォルト ポートは、1645 です。

f. Server Accounting Port：ユーザ アカウンティング用のサーバ ポート。デフォルト ポートは、1646 です。

g. Retry Interval：接続を試行するまでに待機する秒数を選択します。デフォルト設定は、10 秒です。この例では、デフォルト設定を使用します。

h. Server Secret Key：暗号鍵を入力します。大文字と小文字が区別されます。この例では、鍵は *x5*zbrct* です。

i. Common Password：RADIUS の共通パスワードを入力します。この例では、パスワードは *12345678* です。

j. ACL Netmask Convert：Detect Automatically、Standard、または Wildcard を選択します。この例では、**Standard** を選択します。

ステップ 4　設定を指定した後、**OK** および **Apply** をクリックします。

同じ手順を実行して、残りの 2 つのホストを AAA サーバ グループに追加します。

外部認証を使用するリモート アクセス用のトンネル グループの追加

最後に、トンネル グループを追加します。この例では、トンネル グループの名前は ACSRadiusGroup です。AAA サーバ グループの名前は、ACSRadiusServers です。

CLI コマンドを使用した手順

次のコマンドは、トンネル グループの名前を指定し、トンネル グループの一般アトリビュート モードにアクセスし、トンネル グループを認証グループに割り当てます。最後の 2 つのコマンドは、IPSec アトリビュート モードに移行し、リモート アクセス認証用の事前共有鍵を設定します。

```
hostname(config)# tunnel-group ACSRadiusGroup type ipsec_ra
hostname(config)# tunnel-group ACSRadiusGroup general-attributes
hostname(config-general)# address-pool IPPool2
hostname(config-general)# authentication-server-group ACSRadiusServers
hostname(config)# tunnel-group ACSRadiusGroup ipsec-attributes
hostname(config-ipsec)# pre-shared k*5$h9s%
```

ASDM を使用した手順

ASDM を使用して、外部認証を使用するリモート アクセス用のトンネル グループを追加する手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Tunnel Group パネルで **Add** をクリックし、**IPSec for Remote Access** を選択します。ASDM に Add Tunnel Group ダイアログボックスが表示され、General タブと Basic タブが示されます。

ステップ 2　Name フィールドにこのトンネル グループの名前を入力します。この例では、名前は ACSRadiusGroup です。

ステップ 3　General タブで **AAA** タブをクリックします。

ステップ 4　Authentication Server Group リストからサーバ 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 ACSRadiusServers です（「サーバ グループの追加」を参照してください）。

ステップ 5　このリモート アクセス トンネル グループの IPSec アトリビュートを設定するには、**IPSec** タブをクリックし、Pre-shared Key フィールドに暗号鍵を入力します。この例では、事前共有鍵は *k*5$h9s%* です。次に **OK** および **Apply** をクリックします。