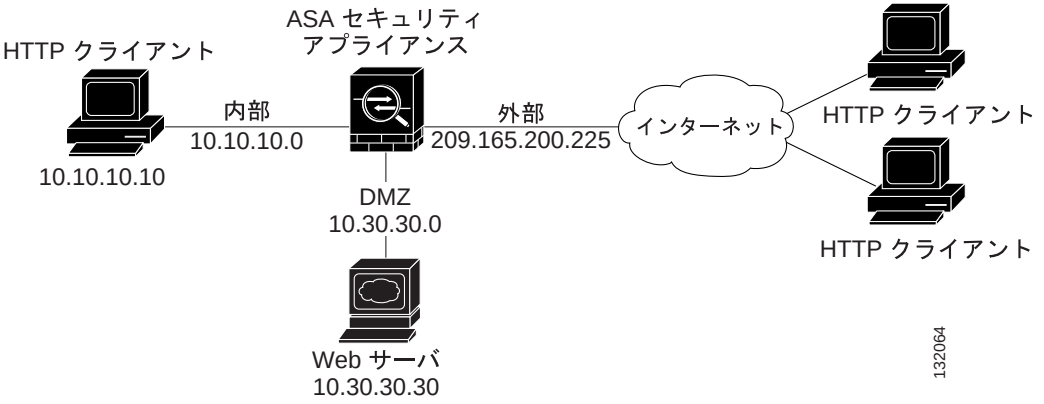
シナリオ：DMZ の設定

非武装地帯（DMZ）とは、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間の中立ゾーンにある区別されたネットワークです。このネットワーク トポロジの例は、適応型セキュリティ アプライアンスのほとんどの DMZ 実装と類似しています。Web サーバは DMZ インターフェイスにあり、内部ネットワークと外部ネットワークの両方から HTTP クライアントがセキュアに Web サーバにアクセスできます。

図 6-1 では、内部ネットワークの HTTP クライアント（10.10.10.10）が DMZ Web サーバ（10.30.30.30）との HTTP 通信を開始します。DMZ Web サーバへの HTTP アクセスは、インターネット上のすべてのクライアントに提供されます。その他のすべての通信は拒否されます。ネットワークは、10.30.30.50 ～ 10.30.30.60 のアドレスの IP プールを使用するように設定されます（IP プールは、DMZ インターフェイスで使用できる IP アドレスの範囲です）。

図 6-1　DMZ の設定シナリオのネットワーク レイアウト



DMZ Web サーバはプライベート DMZ ネットワークにあるため、プライベート IP アドレスをパブリック（ルーティング可能な）IP アドレスに変換する必要があります。このパブリック アドレスを使用して、外部クライアントは、インターネット上の任意のサーバにアクセスするときと同じ方法で DMZ Web サーバにアクセスできます。

図 6-1 で示す DMZ 設定シナリオには、パブリックに使用可能な 2 つのルーティング可能 IP アドレスがあります。1 つは適応型セキュリティ アプライアンスの外部インターフェイス（209.165.200.225）で、もう 1 つは DMZ Web サーバのパブリック IP アドレス（209.165.200.226）です。次の手順で、ASDM を使用して、HTTP クライアントと Web サーバの間でセキュアな通信を行うように、適応型セキュリティ アプライアンスを設定する方法を示します。

この DMZ のシナリオでは、適応型セキュリティ アプライアンスには、設定済みの外部インターフェイス **dmz** があるものとします。DMZ 用に適応型セキュリティ アプライアンスインターフェイスをセットアップするには、Startup Wizard を使用します。セキュリティ レベルが 0 ～ 100 に設定されていることを確認します（一般的な値は 50 です）。

DMZ のシナリオの実装

次の項で、図 6-1 で示したシナリオのパラメータ例を使用して、DMZ 配置で適応型セキュリティ アプライアンスを設定する方法を示します。

必要な情報

この設定手順を開始する前に、次の情報を収集します。

- パブリック　ネットワーク上のクライアントが使用できるようにする　DMZ 内のサーバ（このシナリオでは Web サーバ）の内部 IP アドレス
- DMZ 内のサーバが使用する外部 IP アドレス（パブリック ネットワーク上のクライアントは、外部 IP アドレスを使用して DMZ 内のサーバにアクセスします）
- 発信トラフィックで、内部 IP アドレスと置き換えるクライアント IP アドレス（発信クライアント トラフィックはこのアドレスから発信されたように見え、内部 IP アドレスは公開されません）

DMZ 配置用のセキュリティ アプライアンスの設定

この手順で、DMZ 内の Web サーバを保護するように適応型セキュリティ アプライアンスを設定するために、実行する必要がある設定手順を説明します。この手順では、配置例として図 6-1 で示すネットワーク トポロジを使用します。次の手順が含まれます。

1. ネットワーク変換用の IP プールの設定
2. プライベート ネットワークでのアドレス変換の設定
3. DMZ Web サーバの外部アイデンティティの設定
4. DMZ Web サーバへの HTTP アクセスの提供

ネットワーク変換用の IP プールの設定

内部 HTTP クライアント（10.10.10.10）が DMZ ネットワークの Web サーバ（10.30.30.30）にアクセスするには、DMZ インターフェイス用の IP アドレスのプール（10.30.30.50 ～ 10.30.30.60）を定義する必要があります。同様に、内部 HTTP クライアントがパブリック ネットワーク上の任意のデバイスと通信するには、外部インターフェイス用の IP プール（209.165.200.225）が必要です。ASDM を使用すると、IP プールを効率的に管理でき、保護されたネットワーク クライアントとインターネット上のデバイスとのセキュアな通信が容易になります。

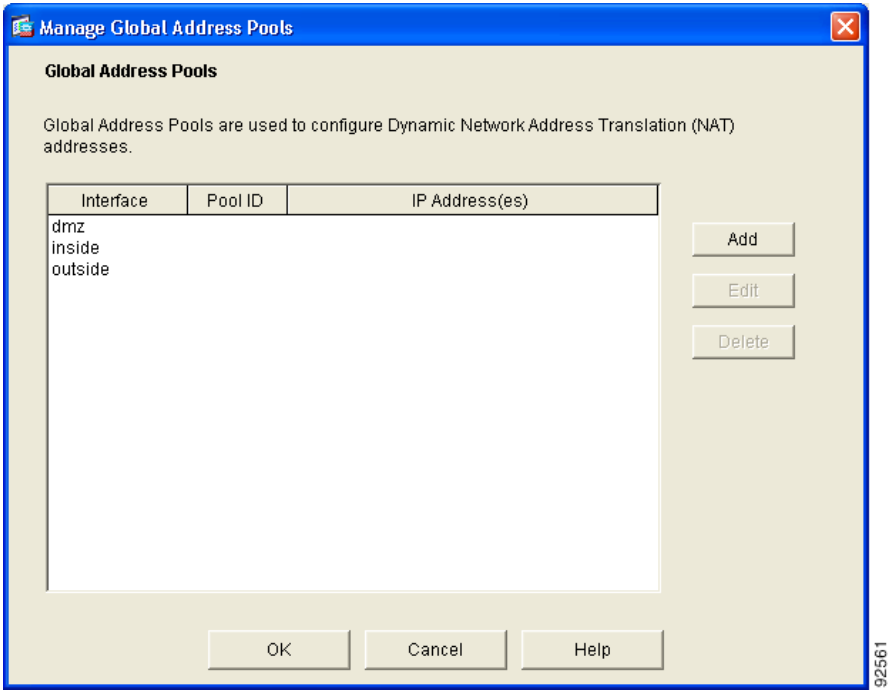
ネットワーク変換用に IP プールを設定するには、次の手順を実行します。

ステップ 1　Web ブラウザのアドレス フィールドに、工場出荷時のデフォルト IP アドレス **https://192.168.1.1/admin/** を入力して、ASDM を起動します。

（注）　「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

ステップ 2　ASDM ウィンドウの上部で **Configuration** タブをクリックし、ASDM ウィンドウの左側で **NAT** 機能をクリックします。

ステップ 3　ASDM ウィンドウの下部で **Manage Pools** をクリックします。Manage Global Address Pools ダイアログボックスが表示され、グローバル アドレス プールの追加または編集ができます。

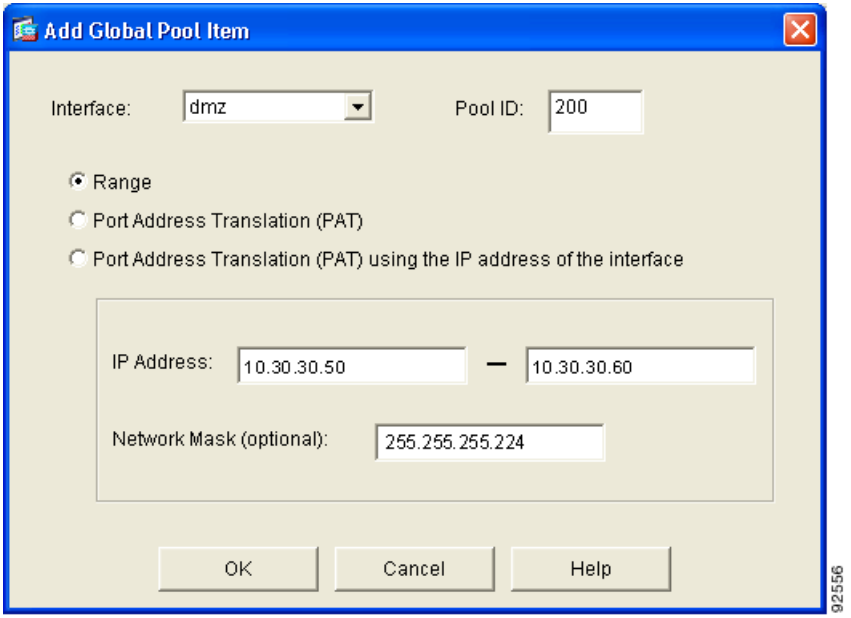


（注）　ほとんどの設定で、グローバル プールはよりセキュアでない（パブリックな）インターフェイスに追加されます。

ステップ 4　Manage Global Address Pools ダイアログボックスで、次の操作を実行します。

a. **dmz** インターフェイス（この手順を開始する前に、Startup Wizard で設定済み）をクリックします。

b. **Add** をクリックします。Add Global Pool Item ダイアログボックスが表示されます。



ステップ 5　Add Global Pool Item ダイアログボックスで、次の操作を実行します。

a. Interface ドロップダウン リストで、**dmz** をクリックします。

b. **Range** をクリックして、IP アドレスの範囲を入力します。

c. DMZ インターフェイスの IP アドレスの範囲を入力します。このシナリオでは、範囲は 209.165.200.230 ～ 209.165.200.240 です。

d. 一意の Pool ID を入力します。このシナリオでは、Pool ID は 200 です。

e. **OK** をクリックして、Manage Global Address Pools ダイアログボックスに戻ります。

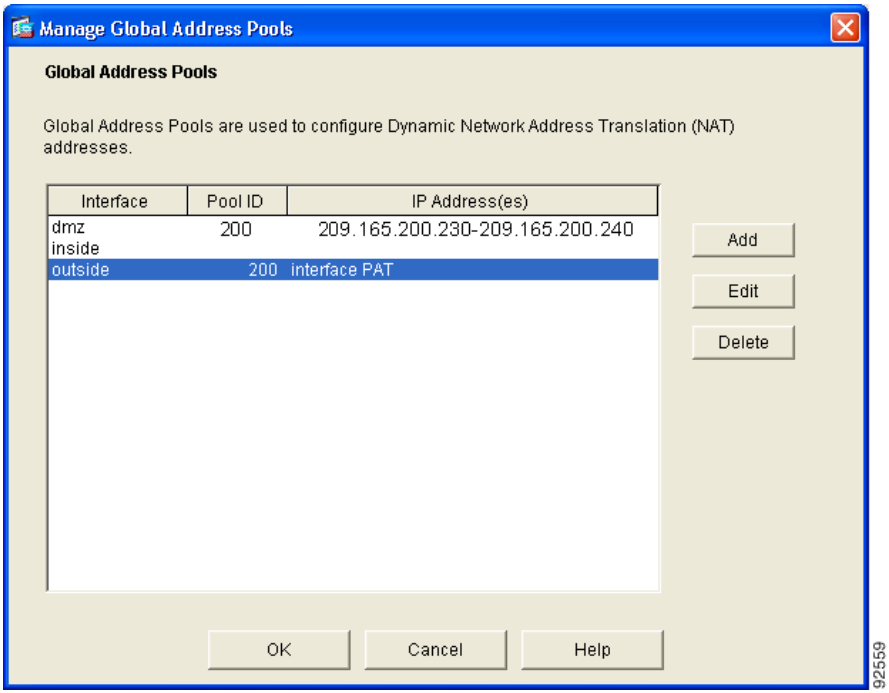
（注） DMZ インターフェイスに使用できる IP アドレスが制限されている場合は、**Port Address Translation (PAT)** または **Port Address Translation (PAT) using the IP address of the interface** をクリックすることもできます。

ステップ 6　Manage Global Address Pools ダイアログボックスで、次の操作を実行します。

a. **outside** インターフェイスをクリックします。
b. **Add** をクリックします。

ステップ 7　Add Global Pool Item ダイアログボックスが表示されます。

a. Interface ドロップダウン リストで、**outside** をクリックします。
b. **Port Address Translation (PAT) using the IP address of the interface** をクリックします。
c. ステップ 5d と同じ方法で、このプールに同じ Pool ID を割り当てます（このシナリオでは、Pool ID は 200 です）。
d. **OK** をクリックします。表示される設定は、次のようになります。



ステップ 8　設定値が正しいことを確認します。

a. **OK** をクリックします。

b. ASDM のメイン ウィンドウで **Apply** をクリックします。

（注） 使用できるパブリック IP アドレスは 2 つだけで、1 つは DMZ サーバ用に予約されているため、内部 HTTP クライアントから発信されたすべてのトラフィックは、外部インターフェイス IP アドレスを使用して適応型セキュリティ アプライアンスから送出されます。この設定によって、内部クライアントからのトラフィックがインターネットとの間でルーティングされます。

プライベート ネットワークでのアドレス変換の設定

ネットワーク アドレス変換（NAT）は、適応型セキュリティ アプライアンスの 2 つのインターフェイス間で交換されるネットワーク トラフィックの発信元 IP アドレスを置き換えます。この変換によって、内部 IP アドレスをパブリック ネットワークに公開せずに、パブリック ネットワークを通じたルーティングができます。

ポート アドレス変換（PAT）は、NAT 機能の拡張で、プライベート ネットワーク上の複数のホストをパブリック ネットワーク上の単一の IP アドレスにマッピングします。PAT は、使用できるパブリック IP アドレスの数が制限されている小規模から中規模のビジネスに不可欠です。

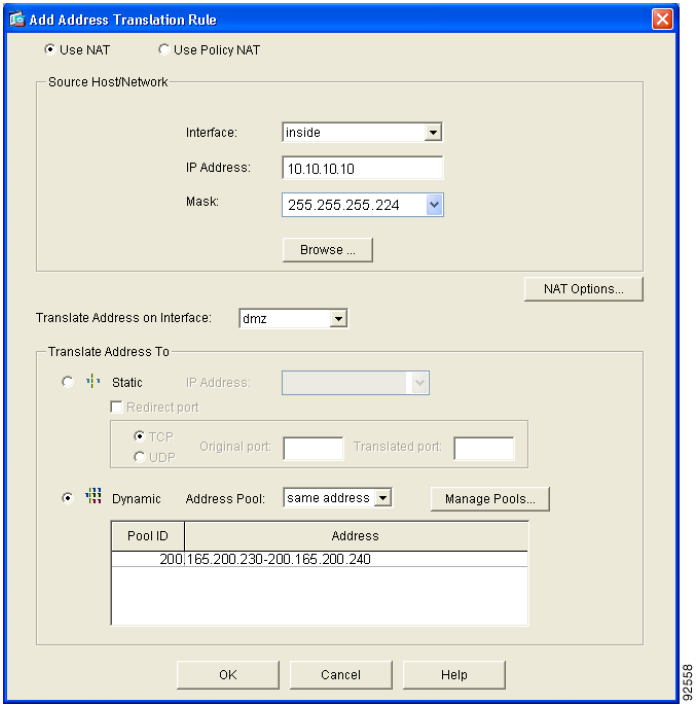
内部 HTTP クライアントの内部インターフェイスと DMZ インターフェイスとの間で NAT を設定するには、ASDM のメイン ウィンドウから、次の手順を実行します。

ステップ 1　ASDM ウィンドウの上部で **Configuration** タブをクリックします。

ステップ 2　ASDM ウィンドウの左側で **NAT** タブをクリックします。

ステップ 3　**Translation Rules** をクリックし、ASDM ウィンドウの右側の **Add** をクリックします。

ステップ 4　Add Address Translation Rule ダイアログボックスで、**Use NAT** チェックボックスをオンにし、**inside** インターフェイスをクリックします。



ステップ 5　内部クライアントの IP アドレスを入力します。このシナリオでは、IP アドレスは **10.10.10.10** です。

ステップ 6　Mask ドロップダウン リストで、**255.255.255.224** を選択します。

ステップ 7　Translate Address on Interface ドロップダウン リストで、DMZ インターフェイスを選択します。

ステップ 8　Translate Address To 領域で、**Dynamic** をクリックします。

ステップ 9　Address Pools ドロップダウン リストで、**200** をクリックします。

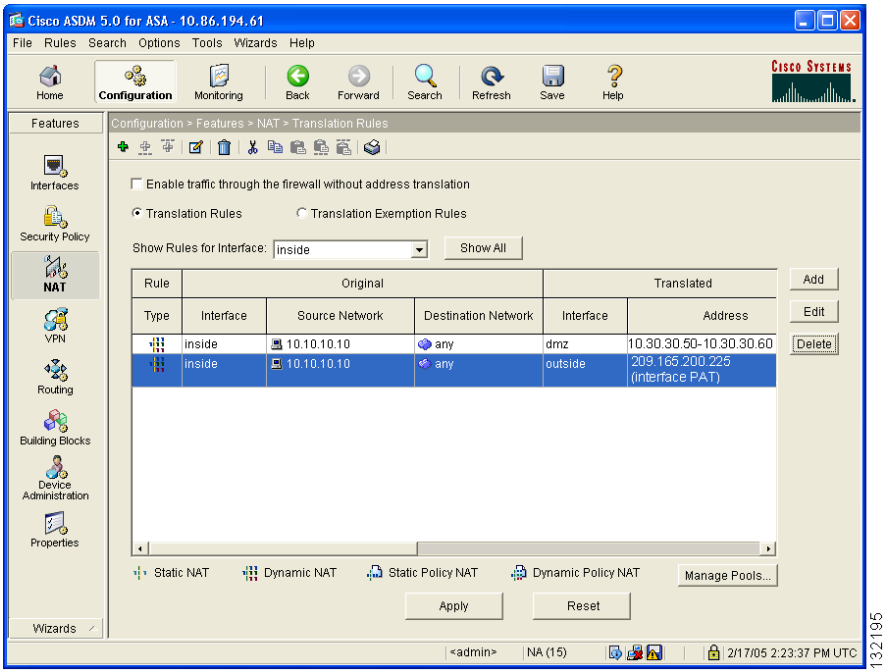
ステップ 10　**OK** をクリックします。

ステップ 11　続行するかどうかを尋ねるダイアログボックスが表示されます。**Proceed**　をクリックします。

ステップ 12　NAT Translation Rules ウィンドウで、表示された設定が正しいことを確認します。

ステップ 13　**Apply** をクリックして、適応型セキュリティ アプライアンスの設定変更を完了します。

表示される設定は、次のようになります。



DMZ Web サーバの外部アイデンティティの設定

DMZ Web サーバは、インターネット上のすべてのホストから簡単にアクセスできる必要があります。この設定では、Web サーバの IP アドレスを変換して、外部 HTTP クライアントが適応型セキュリティ アプライアンスを認識せずにアクセスできるように、Web サーバがインターネット上にあるように見せる必要があります。次の手順を実行して、Web サーバの IP アドレス（10.30.30.30）をパブリック IP アドレス（209.165.200.225）に、スタティックにマッピングします。

ステップ 1　ASDM ウィンドウの上部で **Configuration** タブをクリックします。

ステップ 2　ASDM ウィンドウの左側で **NAT** タブをクリックします。

ステップ 3　**Translation Rules** をクリックし、ウィンドウの右側の **Add** をクリックします。

ステップ 4　インターフェイスのドロップダウン リストで、外部 **dmz** インターフェイスをクリックします。

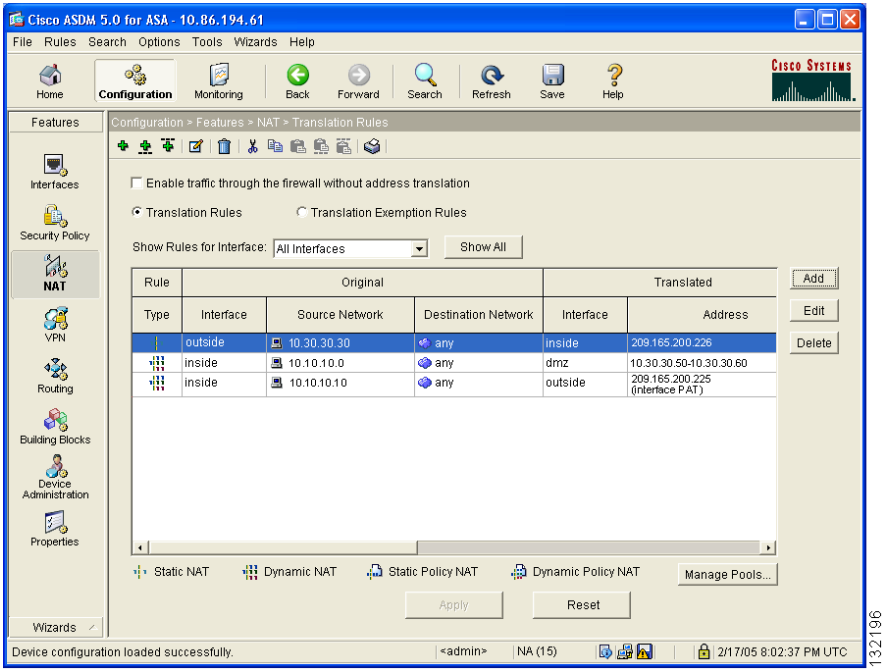
ステップ 5　Web サーバの **IP アドレス**（10.30.30.30）を入力します。

ステップ 6　Mask ドロップダウン リストで、**255.255.255.224** をクリックし、**Static** をクリックします。

ステップ 7　Web サーバの外部 IP アドレス（209.165.200.226）を入力します。**OK** をクリックします。

ステップ 8　入力した値を確認し、**Apply** をクリックします。

表示される設定は、次のようになります。



DMZ Web サーバへの HTTP アクセスの提供

デフォルトでは、適応型セキュリティ アプライアンスはパブリック ネットワークから発信されたすべてのトラフィックを拒否します。適応型セキュリティ アプライアンスでアクセス コントロール規則を作成して、パブリック ネットワークからの特定の種類のトラフィックが適応型セキュリティ アプライアンスを通過して、DMZ のリソースに到達できるようにする必要があります。

インターネット上の任意のクライアントが DMZ 内の Web サーバにアクセスできるように、HTTP トラフィックによる適応型セキュリティ アプライアンスの通過を許可するアクセス コントロール規則を設定するには、次の手順を実行します。

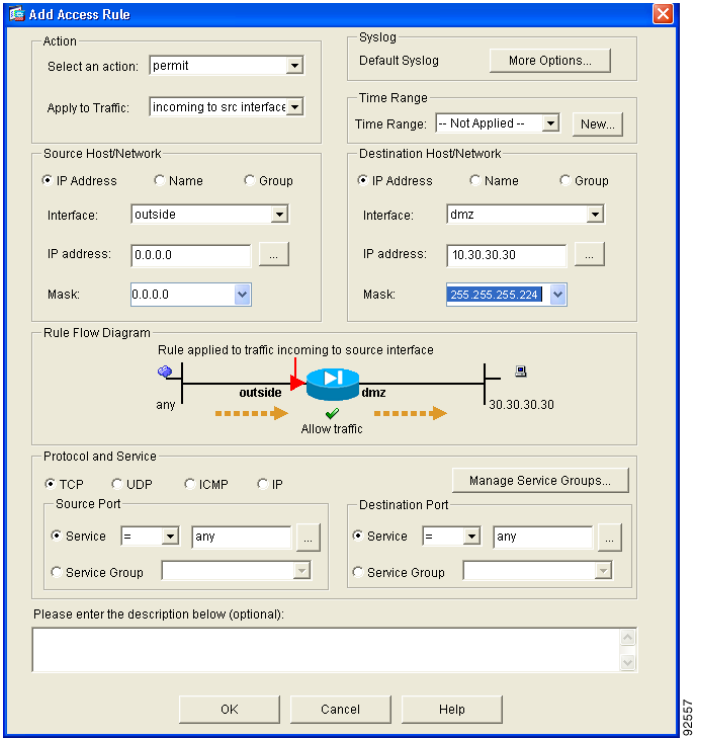
ステップ 1　ASDM ウィンドウで、次の手順を実行します。

a. **Configuration** をクリックします。
b. ASDM ウィンドウの左側で **Security Policy** をクリックします。
c. テーブル内で、**Add** をクリックします。

ステップ 2　Add Access Rule ダイアログボックスで、次の手順を実行します。

a. Action 領域のドロップダウン リストで **permit** をクリックし、トラフィックが適応型セキュリティ アプライアンスを通過できるようにします。
b. Source Host/Network 領域で、**IP Address** をクリックします。
c. Interface ドロップダウン リストで、**outside** をクリックします。
d. Source Host/Network 情報の IP アドレスを入力します（すべてのホストまたはネットワークから発信されたトラフィックを許可するには、0.0.0.0 を使用します）。
e. Destination Host/Network 領域で、**IP Address** をクリックします。
f. Interface ドロップダウン リストで、**dmz** インターフェイスをクリックします。
g. IP address フィールドに、宛先ホストまたはネットワーク（Web サーバなど）の IP アドレスを入力します（このシナリオでは、Web サーバの IP アドレスは 10.30.30.30 です）。
h. Mask ドロップダウン リストで、**255.255.255.224** をクリックします。

（注）　または、どちらの場合も、対応する **Browse** ボタンをクリックして、ホストまたはネットワークをクリックすることもできます。



ステップ 3　許可するトラフィックの種類を指定します。

（注）　HTTP トラフィックは常に、任意の TCP 発信元ポート番号から固定された宛先 TCP ポート番号 80 に誘導されます。

a. Protocol and Service 領域で、**TCP** をクリックします。

b. Source Port 領域の **Service** ドロップダウン リストで、「=」（等号）をクリックします。

c. 省略記号（**...**）のラベルが付いたボタンをクリックし、オプションをスクロールし、**Any** をクリックします。

d. Destination Port 領域の **Service** ドロップダウン リストで、「=」（等号）をクリックします。

e. 省略記号（**...**）のラベルが付いたボタンをクリックし、オプションをスクロールし、**HTTP** をクリックします。

f. **OK** をクリックします。

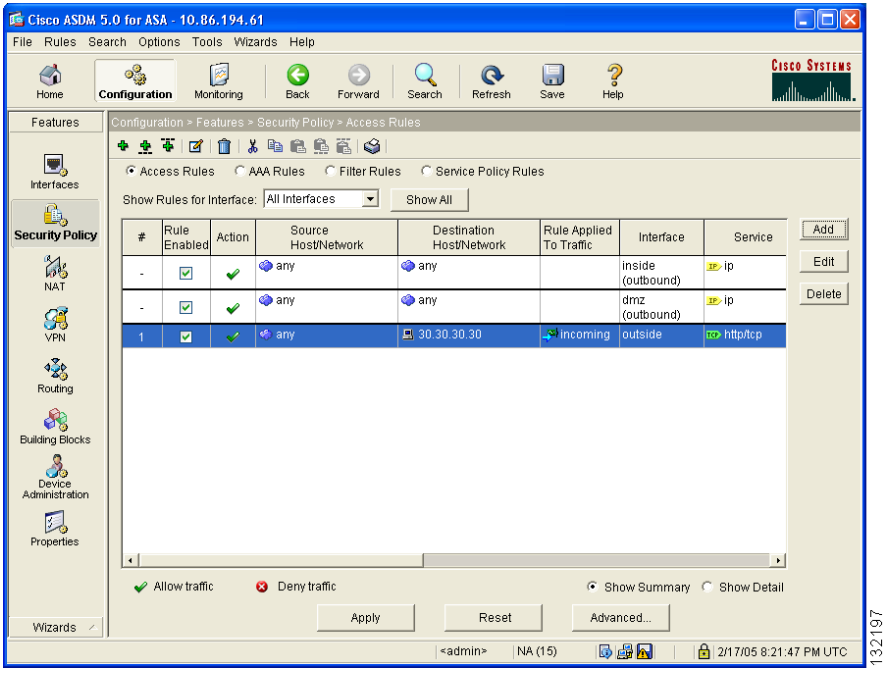
（注） ACL によるシステム メッセージのロギングなど、その他の機能については、ウィンドウの上部の **More Options** をクリックしてください。アクセス規則の名前は、下部のダイアログボックスで指定できます。

g. 入力した情報が正しいことを確認し、**OK** をクリックします。

（注） 指定された宛先アドレスは DMZ Web サーバのプライベート アドレス（10.30.30.30）ですが、209.165.200.225 に送信されたインターネット上のすべてのホストからの HTTP トラフィックが、適応型セキュリティ アプライアンスを通過できます。アドレス変換（10.30.30.30 = 209.165.200.225）によって、トラフィックが許可されます。

h. ASDM のメイン ウィンドウで **Apply** をクリックします。

表示される設定は、次のようになります。



プライベート ネットワークとパブリック ネットワークの両方の HTTP クライアントが、DMZ Web サーバにセキュアにアクセスできます。

次の手順

DMZ 内の Web サーバを保護する目的で適応型セキュリティ アプライアンスを配置するだけの場合は、これで初期設定は終わりです。次の追加の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
リモートアクセス VPN の設定	第 7 章「シナリオ：リモートアクセス VPN の設定」
サイトツーサイト VPN の設定	第 8 章「シナリオ：サイトツーサイト VPN の設定」

次の手順