シナリオ：DMZ の設定

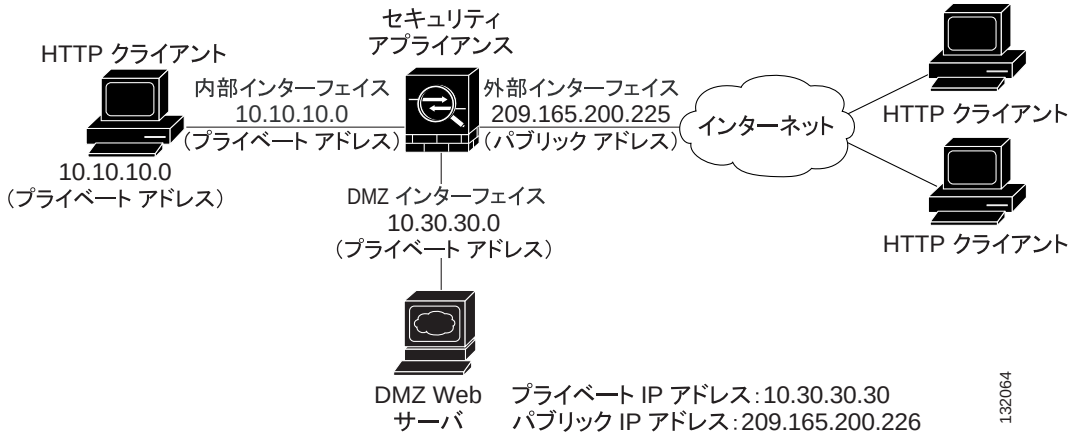
この章では、非武装地帯（DMZ）にあるネットワーク リソースを保護するために適応型セキュリティ アプライアンスが使用される設定シナリオについて説明します。DMZ とは、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間の中立ゾーンにある区別されたネットワークです。

この章は、次の項で構成されています。

DMZ ネットワーク トポロジの例

図 6-1 で示すネットワーク トポロジは、適応型セキュリティ アプライアンスのほとんどの DMZ 実装の代表的な例です。

図 6-1　DMZ の設定シナリオのネットワーク レイアウト



このシナリオの例には、次の特徴があります。

- Web サーバは、適応型セキュリティ アプライアンスの DMZ インターフェイス上にあります。
- プライベート ネットワーク上の HTTP クライアントは、DMZ の Web サーバにアクセスでき、またインターネット上のデバイスとも通信できます。
- インターネット上のクライアントは、DMZ Web サーバへの HTTP アクセスを許可され、その他のトラフィックはすべて拒否されます。
- ネットワークには、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。

図 6-2 は、プライベート ネットワークから DMZ Web サーバとインターネットの両方への HTTP 要求の発信トラフィック フローを示しています。

図 6-2　プライベート ネットワークからの発信 HTTP トラフィック フロー

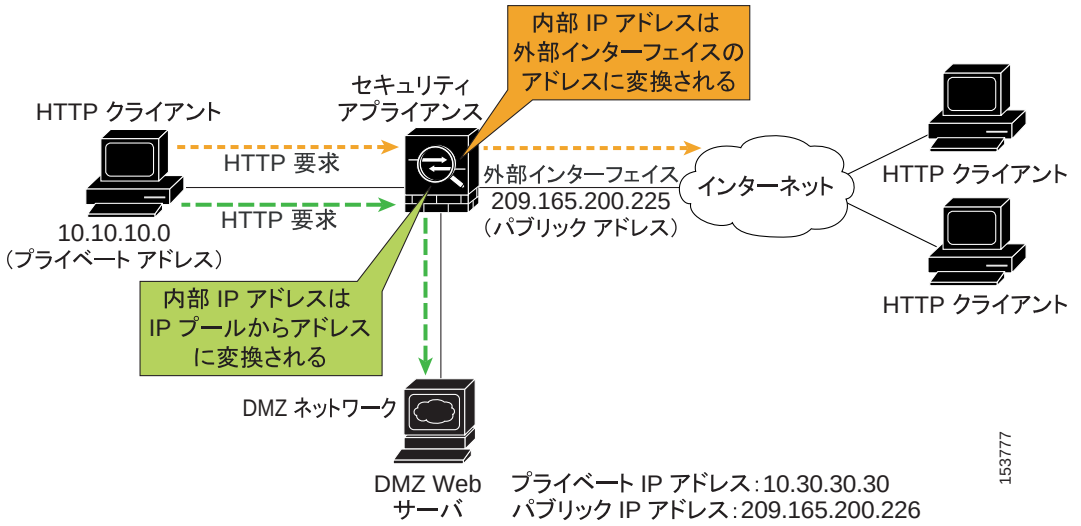


図 6-2 では、内部のクライアントから発信され、DMZ Web サーバとインターネット上のデバイスの両方に送信される HTTP トラフィックが適応型セキュリティ アプライアンスによって許可されます。トラフィックの通過を許可するために、適応型セキュリティ アプライアンス設定には次の要素が含まれています。

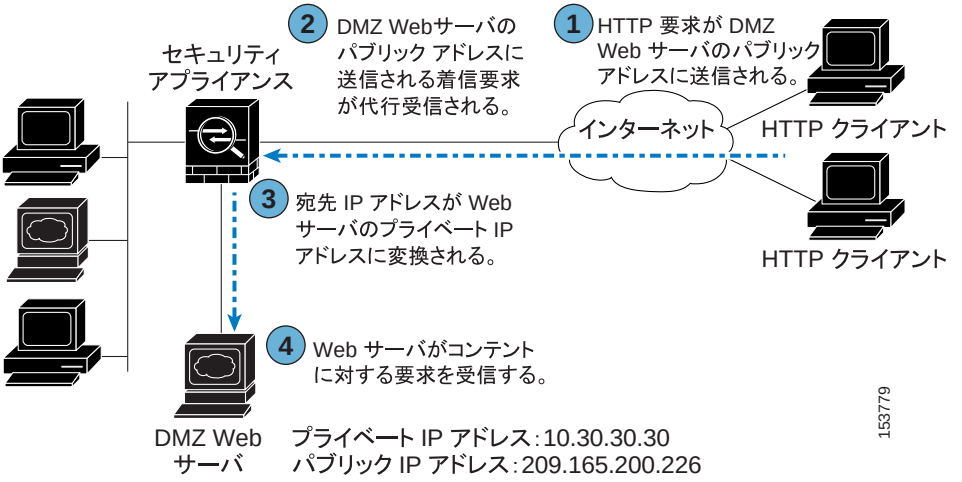
- アクセス コントロール規則（DMZ Web サーバとインターネット上のデバイスに送信されるトラフィックを許可します）
- アドレス変換規則（プライベート IP アドレスをインターネットから見えないように変換します）

  DMZ Web サーバに送信されるトラフィックの場合、プライベート IP アドレスは IP プールからアドレスに変換されます。

  インターネットに送信されるトラフィックの場合、プライベート IP アドレスは適応型セキュリティ アプライアンスのパブリック IP アドレスに変換されます。発信トラフィックは、このアドレスから発信されたように見えます。

図 6-3 は、インターネットから発信され、DMZ Web サーバのパブリック IP アドレスに送信される HTTP 要求を示しています。

図 6-3　インターネットからの着信 HTTP トラフィック フロー



着信トラフィックに DMZ Web サーバへのアクセスを許可するために、適応型セキュリティ アプライアンス設定には次の要素が含まれています。

- アドレス変換規則（DMZ Web サーバのパブリック IP アドレスを DMZ Web サーバのプライベート IP アドレスに変換します）
- アクセス コントロール規則（DMZ Web サーバに送信される着信 HTTP トラフィックを許可します）

この設定の作成手順は、この章の残りの部分で詳しく説明します。

DMZ 配置用のセキュリティ アプライアンスの設定

この章では、ASDM を使用して、図 6-1 で示す設定シナリオの適応型セキュリティ アプライアンスを設定する方法について説明します。手順で使用するサンプル パラメータは、シナリオに基づいています。

この設定手順では、内部インターフェイス、DMZ インターフェイス、および外部インターフェイス用に適応型セキュリティ アプライアンスのインターフェイスがすでに設定されていることを前提としています。適応型セキュリティ アプライアンスのインターフェイスをセットアップするには、ASDM の Startup Wizard を使用します。DMZ インターフェイスのセキュリティ 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）。

Startup Wizard の使用方法の詳細については、第 5 章「適応型セキュリティ アプライアンスの設定」を参照してください。

この項では、次のトピックについて取り上げます。

次の各項で、それぞれの手順を実行する方法について詳しく説明します。

設定の要件

この DMZ 配置用に適応型セキュリティ アプライアンスを設定するには、次の設定作業が必要になります。

- DMZ Web サーバへの HTTP アクセスを内部クライアントに提供するために、アドレス変換用の IP アドレスのプールを作成し、そのプールからアドレスを使用するクライアントを特定する必要があります。この作業を完了するには、次の要素を設定する必要があります。
  - DMZ インターフェイス用の IP アドレスのプール。このシナリオでは、IP プールは 10.30.30.50 ～ 10.30.30.60 です。
  - 内部インターフェイス用の動的 NAT 変換規則。この規則には、IP プールからアドレスを割り当てることができるクライアント IP アドレスを指定します。
- 内部クライアントがインターネット上の HTTP リソースおよび HTTPS リソースにアクセスできるようにするために、内部クライアントの実 IP アドレスを、ソース アドレスとして使用できる外部アドレスに変換する規則を作成する必要があります。

  この作業を完了するには、内部 IP アドレスを適応型セキュリティ アプライアンスの外部 IP アドレスに変換する内部インターフェイス用の PAT 変換規則（ポート アドレス変換規則、インターフェイス NAT と呼ばれることもあります）を設定する必要があります。

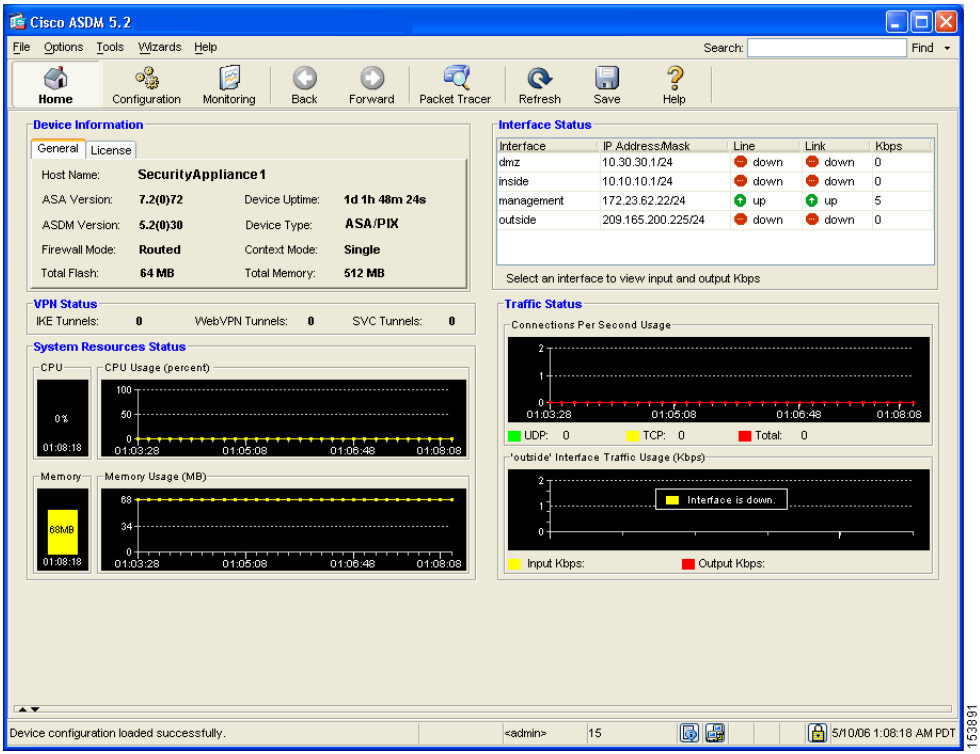
  このシナリオでは、変換される内部アドレスは、プライベート ネットワークのサブネットの内部アドレス（10.10.10.0）です。このサブネットからのアドレスは、適応型セキュリティ アプライアンスのパブリック アドレス（209.165.200.225）に変換されます。
- DMZ Web サーバへの HTTP アクセスを外部クライアントに提供するために、DMZ Web サーバの外部アイデンティティを設定し、またインターネット上のクライアントから発信される HTTP 要求を許可するアクセス規則を設定する必要があります。この作業を完了するには、次の要素を設定する必要があります。
  - 静的 NAT 規則を作成します。この規則は、DMZ Web サーバの実 IP アドレスを単一のパブリック IP アドレスに変換します。このシナリオでは、Web サーバのパブリック アドレスは 209.165.200.226 です。
  - セキュリティ アクセス規則を作成します。この規則は、インターネットからのトラフィックを許可します（DMZ Web サーバのパブリック IP アドレスに送信される HTTP 要求のトラフィックの場合）。

ASDM の起動

ASDM を Web ブラウザで実行するには、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。

ASDM のメイン ウィンドウが表示されます。



ネットワーク アドレス変換用の IP プールの作成

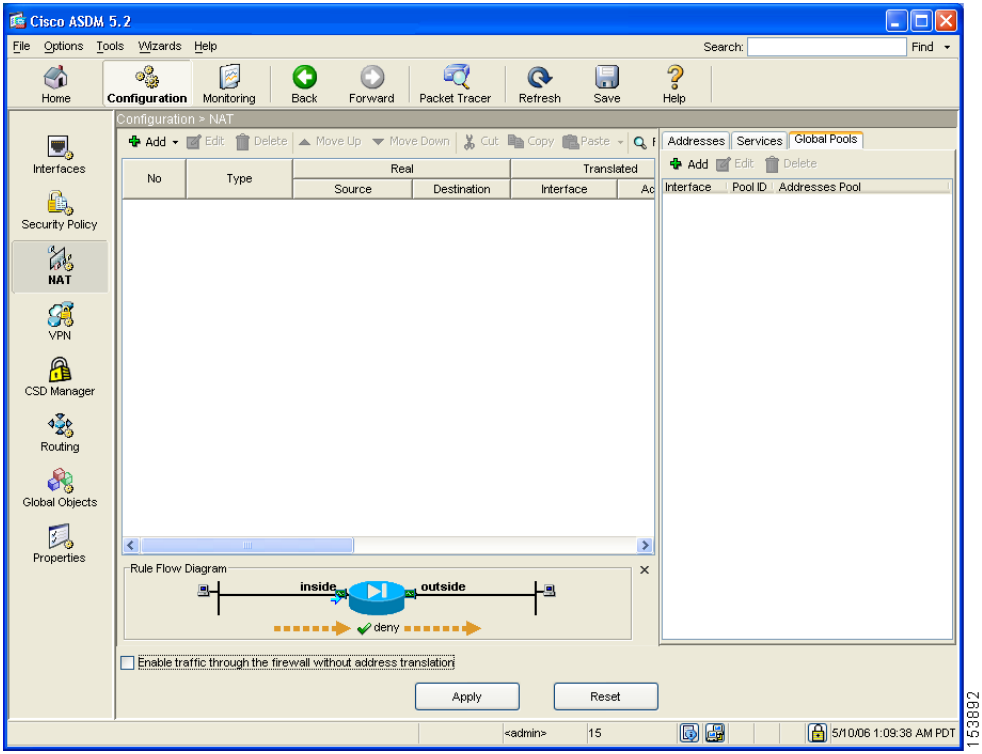
適応型セキュリティ アプライアンスは、ネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）を使用して、内部 IP アドレスが外部に公開されることを防いでいます。この手順では、DMZ インターフェイスおよび外部インターフェイスがアドレス変換に使用できる IP アドレスのプールの作成方法について説明します。

単一の IP プールに NAT と PAT の両方のエントリが含まれることがあり、また複数のインターフェイスのエントリが含まれることもあります。

ネットワーク アドレス変換に使用できる IP アドレスの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　ASDM ウィンドウで、**Configuration** ツールをクリックします。

a. Features ペインで、**NAT** をクリックします。
NAT Configuration 画面が表示されます。

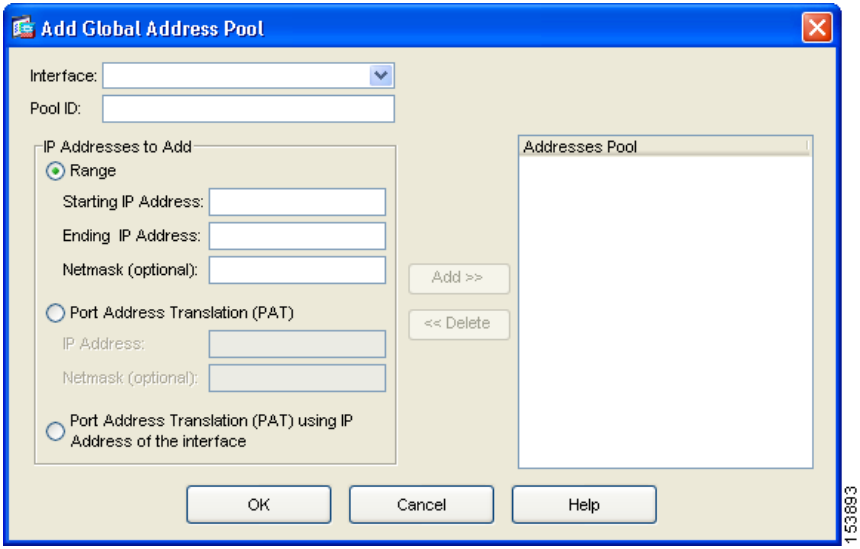


b. 右ペインで、**Global Pools** タブをクリックします。

c. **Add** をクリックして、DMZ インターフェイス用の新しいグローバル プールを作成します。

Add Global Address Pool ダイアログボックスが表示されます。

（注） ほとんどの設定で、IP 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。



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

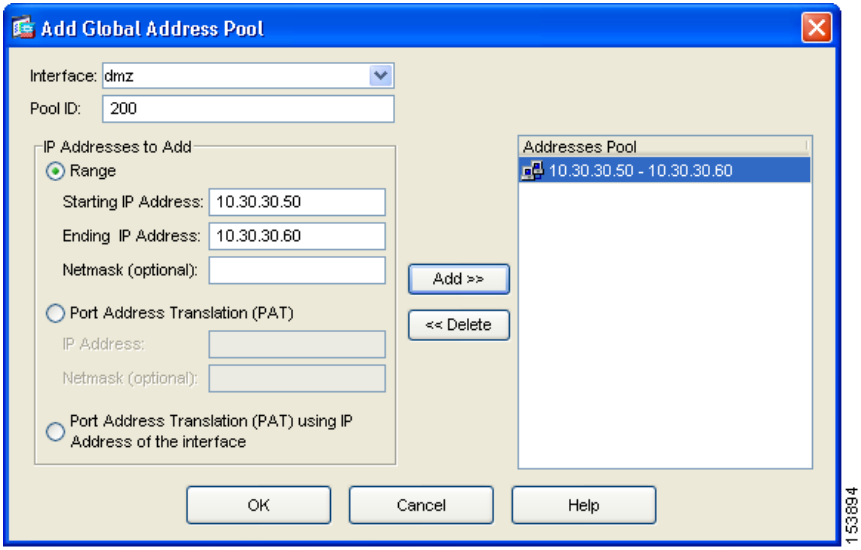
e. 新しい IP プールを作成するには、一意の Pool ID を入力します。このシナリオでは、Pool ID は 200 です。

f. IP Addresses to Add 領域で、DMZ インターフェイスで使用される IP アドレスの範囲を指定します。

- **Range** オプション ボタンをクリックします。
- IP アドレスの範囲の開始値と終了値を入力します。このシナリオでは、IP アドレスの範囲は 10.30.30.50 ～ 10.30.30.60 です。
- （オプション）IP アドレスの範囲のネットマスクを入力します。

g. **Add** をクリックして、この IP アドレスの範囲を Addresses Pool に追加します。

Add Global Pool ダイアログボックスの設定は、次のようになります。



h. **OK** をクリックして、Configuration > NAT ウィンドウに戻ります。

ステップ 2　外部インターフェイスで使用されるアドレスを IP プールに追加します。これらのアドレスはプライベート IP アドレスの変換に使用され、内部クライアントはインターネット上のクライアントとセキュアに通信できます。

このシナリオでは、使用可能なパブリック IP アドレスは制限されています。ポート アドレス変換（PAT）を使用して、次のように多数の内部 IP アドレスを同一のパブリック IP アドレスにマッピングできます。

a. NAT Configuration 画面の右ペインで、**Global Pools** タブをクリックします。

b. Global Pools タブで、**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。

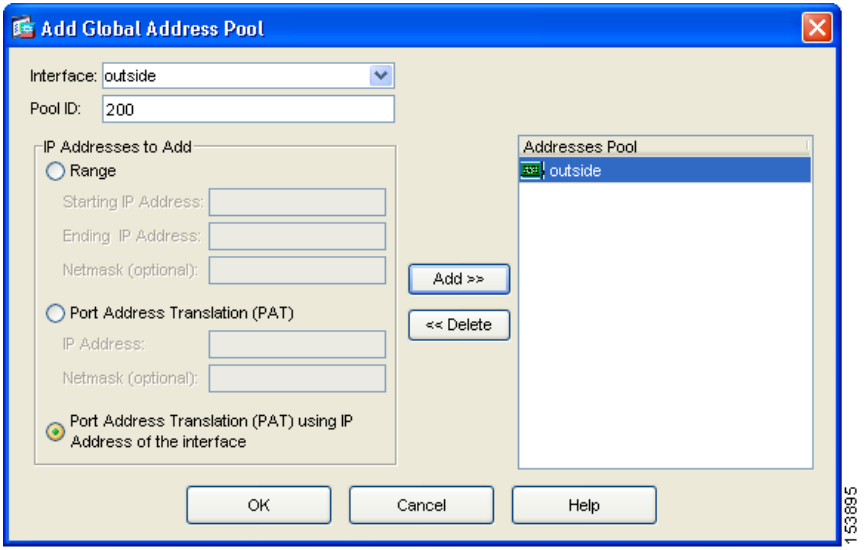
c. Interface ドロップダウン リストで、Outside を選択します。

d. 外部インターフェイス用の Pool ID を指定します。
これらのアドレスは、DMZ インターフェイスで使用されるアドレス プールが含まれる同一の IP プールに追加できます（このシナリオでは、Pool ID は 200 です）。

e. **Port Address Translation (PAT) using IP address of the interface** オプション ボタンをクリックします。

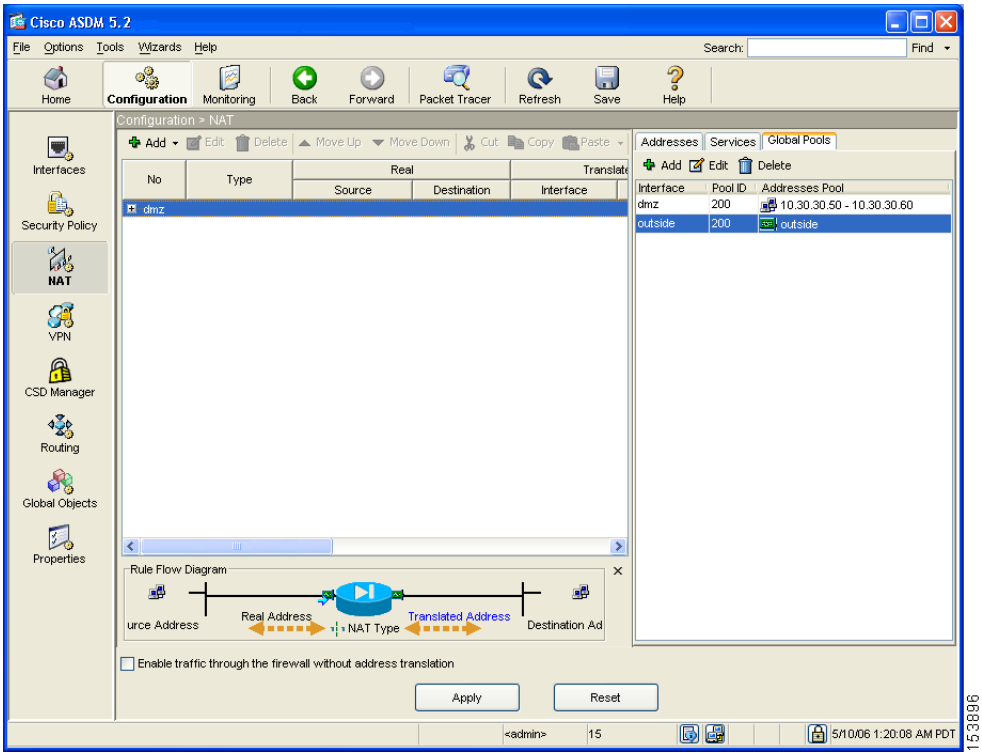
Port Address Translation (PAT) using IP address of the interface オプションを選択した場合、内部ネットワークから発信されたすべてのトラフィックは、外部インターフェイスの IP アドレスを使用して適応型セキュリティ アプライアンスから送出されます。インターネット上のデバイスでは、この 1 つの IP アドレスからすべてのトラフィックが発信されているように見えます。

f. **Add** ボタンをクリックして、この新しいアドレスを IP プールに追加します。



g. **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 3　設定値が正しいことを確認します。

ステップ 4　ASDM のメイン ウィンドウで **Apply** をクリックします。

内部クライアントが DMZ Web サーバと通信するための NAT の設定

前述の手順では、適応型セキュリティ アプライアンスで使用できる IP アドレスのプールを作成して、内部クライアントのプライベート IP アドレスをマスクしました。

この手順では、内部クライアントが DMZ Web サーバとセキュアに通信できるように、このプールからの IP アドレスを内部クライアントに関連付けるネットワーク アドレス変換（NAT）規則を設定します。

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 のメイン ウィンドウで、**Configuration** ツールをクリックします。

ステップ 2　Features ペインで、**NAT** をクリックします。

ステップ 3　Add ドロップダウン リストで、Add Dynamic NAT Rule を選択します。

Add Dynamic NAT Rule ダイアログボックスが表示されます。

ステップ 4　Real Address 領域で、変換する IP アドレスを指定します。このシナリオの場合、内部クライアントのアドレス変換はサブネットの IP アドレスに従って実行されます。

a. Interface ドロップダウン リストで、Inside インターフェイスを選択します。

b. クライアントまたはネットワークの IP アドレスを入力します。このシナリオでは、ネットワークの IP アドレスは 10.10.10.0 です。

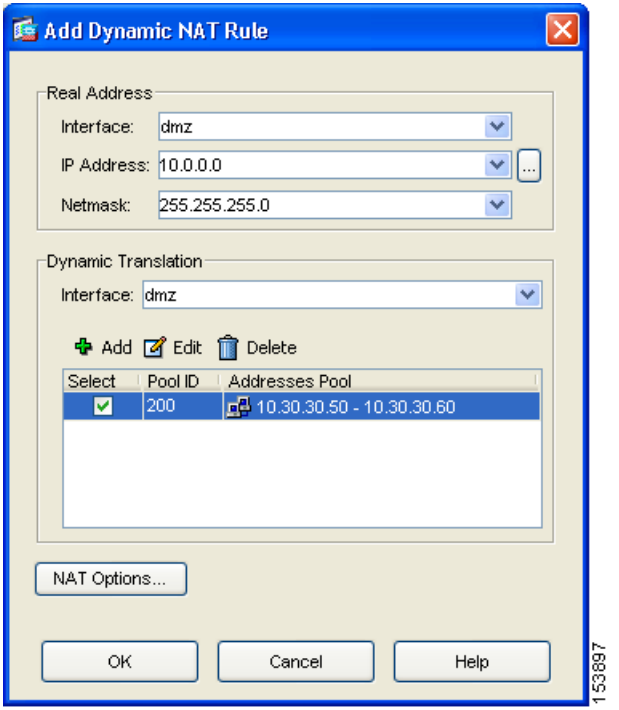
c. Netmask ドロップダウン リストで、ネットマスクを選択します。このシナリオでは、ネットマスクは 255.255.255.0 です。

ステップ 5　Dynamic Translation 領域で、次の手順を実行します。

a. 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。

b. この Dynamic NAT 規則に使用されるアドレス プールを指定するには、Global Pool ID の横にある **Select** チェックボックスをオンにします。このシナリオでは、IP プール ID は 200 です。

このシナリオでは、使用する IP プールはすでに作成されています。作成されていない場合は、**Add** をクリックして、新しい IP プールを作成します。



c. **OK** をクリックして Dynamic NAT Rule を追加し、Configuration > NAT ウィンドウに戻ります。

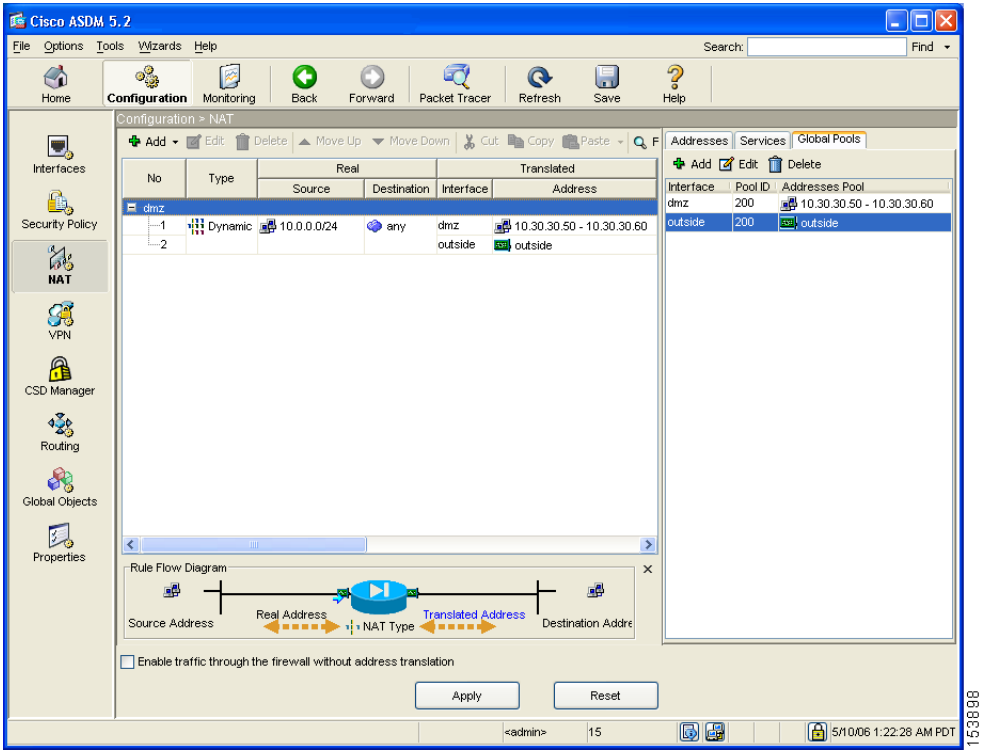
設定画面で、変換規則が予想どおりに表示されることを確認します。

（注） OK をクリックしてこの規則を作成すると、実際には次の 2 つの変換規則が作成されることに注意してください。

- 内部インターフェイスと DMZ インターフェイス間の変換規則。これは、内部クライアントが DMZ Web サーバと通信する際に使用されます。
- 内部インターフェイスと外部インターフェイス間の変換規則。これは、内部クライアントがインターネットと通信する際に使用されます。

変換に使用されるアドレスは両方とも同一の IP プールに存在するので、ASDM は両方の規則を作成できます。

表示される設定は、次のようになります。



ステップ 6　**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。

内部クライアントがインターネット上のデバイスと通信するための NAT の設定

前述の手順では、内部クライアントが DMZ Web サーバとセキュアに通信できるように、IP プールからの IP アドレスを内部クライアントに関連付けるネットワーク アドレス変換（NAT）規則を設定しました。

多くの設定では、内部インターフェイスと外部インターフェイス間の NAT 規則を作成して、内部クライアントがインターネットと通信できるようにする必要もあります。

ただし、このシナリオでは、この規則を明示的に作成する必要はありません。その理由は、アドレス変換に必要な両方のタイプのアドレス（DMZ インターフェイスに使用される IP アドレスと外部インターフェイスに使用される IP アドレスの範囲）が IP プール（プール ID 200）に含まれているためです。したがって、2 番目の変換規則は、ユーザが明示的に作成する代わりに ASDM で作成できます。

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アクセスできる必要があります。この設定では、DMZ Web サーバのプライベート IP アドレスをパブリック IP アドレスに変換して、適応型セキュリティ アプライアンスを認識していない外部 HTTP クライアントにアクセスできるようにする必要があります。Web サーバの実 IP アドレス（10.30.30.30）をパブリック IP アドレス（209.165.200.226）にスタティックにマッピングするには、次の手順を実行します。

ステップ 1　ASDM ウィンドウで、**Configuration** ツールをクリックします。

ステップ 2　Features ペインで、**NAT** をクリックします。

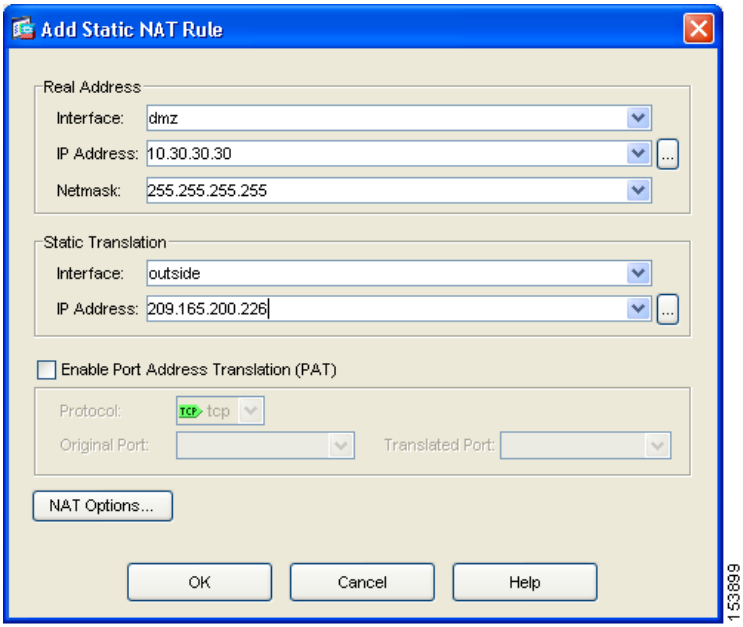
ステップ 3　Add ドロップダウン リストで、Add Static NAT Rule を選択します。Add Static NAT Rule ダイアログボックスが表示されます。

ステップ 4　Real Address 領域で、次のように Web サーバの実 IP アドレスを指定します。

a. 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。

b. DMZ Web サーバの実 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 10.30.30.30 です。

c. Netmask ドロップダウン リストで、ネットマスク 255.255.255.255 を選択します。



ステップ 5　Static Translation 領域で、次のように Web サーバに使用されるパブリック IP アドレスを指定します。

a. Interface ドロップダウン リストで、Outside を選択します。

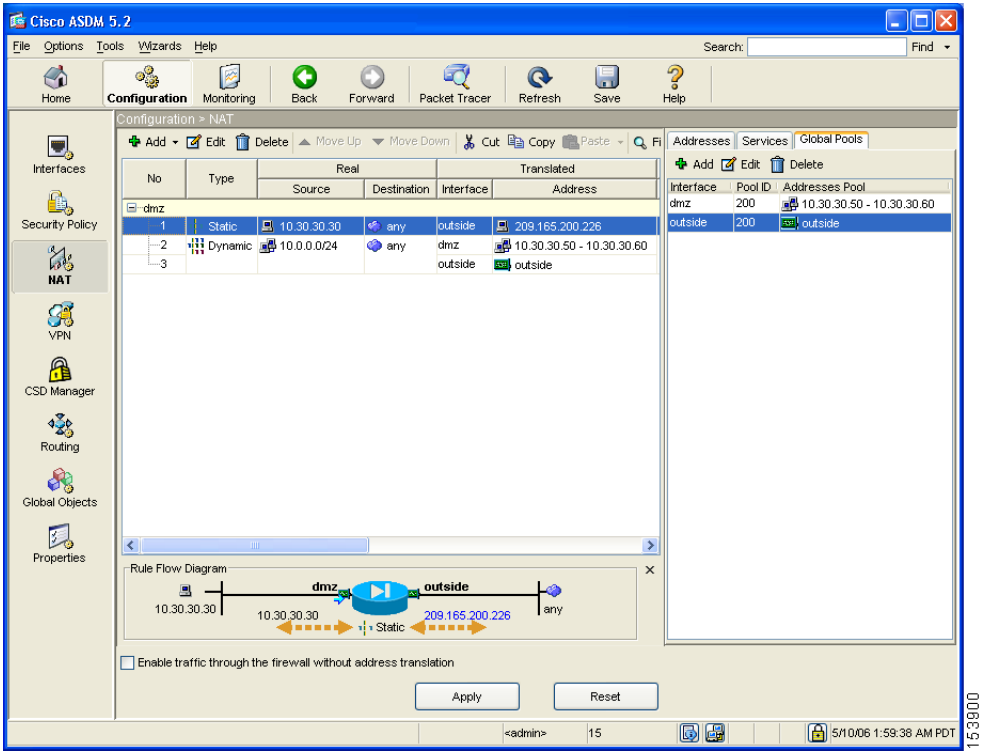
b. IP Address ドロップダウン リストで、DMZ Web サーバのパブリック IP アドレスを選択します。

このシナリオでは、DMZ Web サーバのパブリック IP アドレスは 209.165.200.226 です。

ステップ 6　**OK** をクリックして規則を追加し、Address Translation Rules のリストに戻ります。

この規則は、Web サーバの実 IP アドレス（10.30.30.30）を Web サーバのパブリック IP アドレス（209.165.200.226）にスタティックにマッピングします。

表示される設定は、次のようになります。



ステップ 7　**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。

DMZ Web サーバへのパブリック 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 DMZ のリソースに到達できるようにする必要があります。このアクセス コントロール規則には、トラフィックを処理する適応型セキュリティ アプライアンスのインターフェイス、トラフィックが着信か発信かの区別、トラフィックの発信元と宛先、および許可されるトラフィックのプロトコルとサービスの種類を指定します。

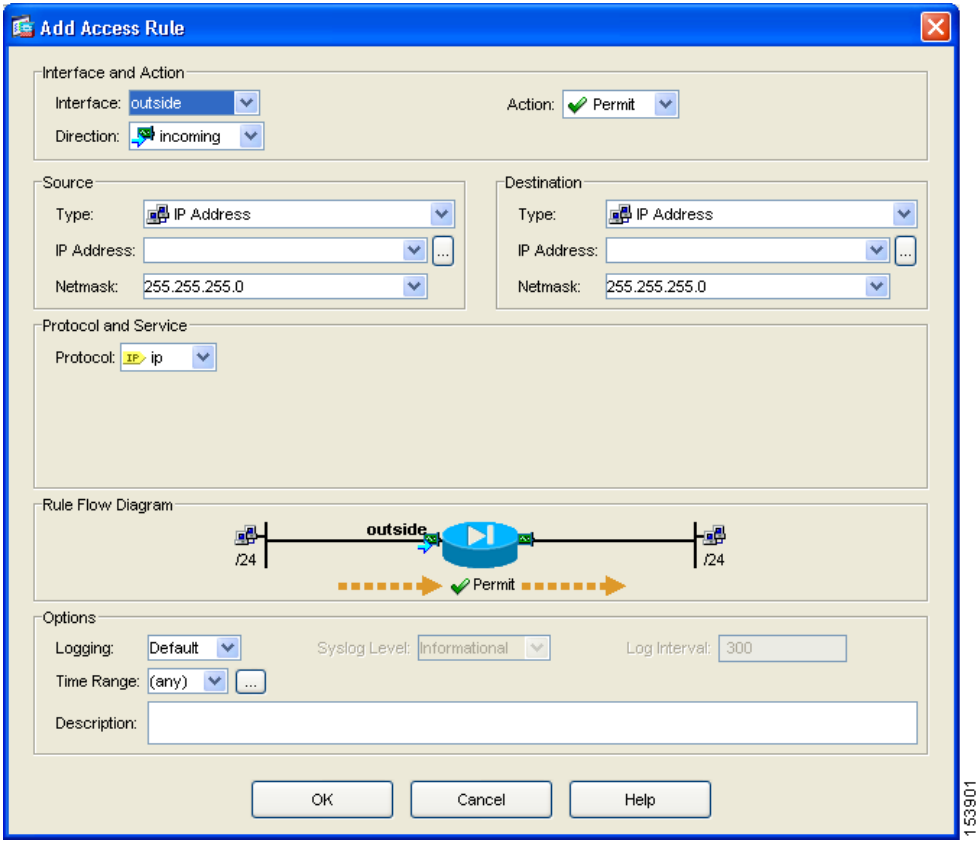
この項では、トラフィックの宛先が DMZ ネットワークの場合に、インターネット上のホストまたはネットワークから発信される着信 HTTP トラフィックを許可するアクセス規則を作成します。パブリック ネットワークから発信されるその他のトラフィックはすべて拒否されます。

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** ツールをクリックします。
b. Features ペインで、**Security Policy** をクリックします。
c. **Access Rules** タブをクリックし、Add プルダウン リストで Add Access Rule を選択します。

   Add Access Rule ダイアログボックスが表示されます。



ステップ 2　Interface and Action 領域で、次の手順を実行します。

a. Interface ドロップダウン リストで、Outside を選択します。
b. Direction ドロップダウン リストで、Incoming を選択します。
c. Action ドロップダウン リストで、Permit を選択します。

ステップ 3　Source 領域で、次の手順を実行します。

a. Type ドロップダウン リストで、IP Address を選択します。

b. 発信元ホストまたは発信元ネットワークの 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）。

あるいは、発信元ホストまたは発信元ネットワークのアドレスが事前設定済みの場合は、IP Address ドロプダウン リストで発信元 IP アドレスを選択します。

c. 発信元 IP アドレスのネットマスクを入力するか、または Netmask ドロップダウン リストで 1 つ選択します。

ステップ 4　Destination 領域で、次の手順を実行します。

a. IP address フィールドに、宛先ホストまたは宛先ネットワーク（Web サーバなど）のパブリック IP アドレスを入力します（このシナリオでは、DMZ Web サーバのパブリック IP アドレスは 209.165.200.226 です）。

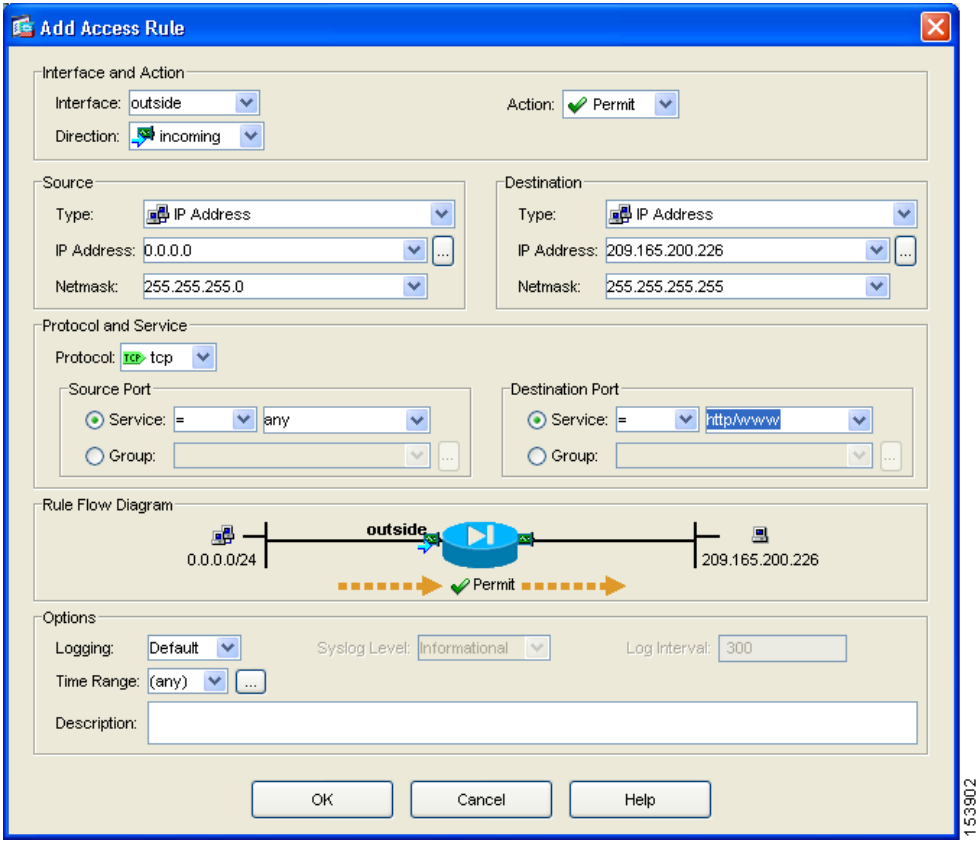
ステップ 5　Protocol and Service 領域で、適応型セキュリティ アプライアンスで許可するトラフィックの種類を指定します。

a. Protocol ドロップダウン リストで、tcp を選択します。

b. Source Port 領域で、**Service** オプション ボタンをクリックし、Service ドロップダウン リストで「=」（等号）を選択し、次のドロップダウン リストで Any を選択します。

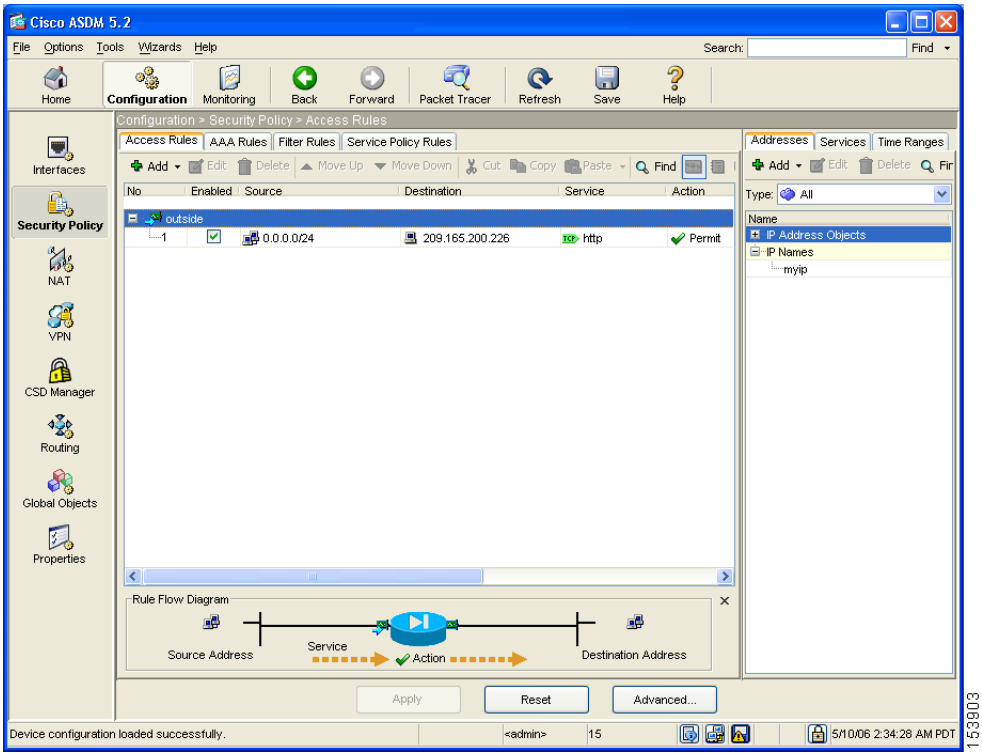
c. Destination Port 領域で、**Service** オプション ボタンをクリックし、Service ドロップダウン リストで「=」（等号）を選択し、次のドロップダウン リストで HTTP/WWW を選択します。

この時点で、Add Access Rule ダイアログボックスのエントリは、次のようになります。



d. **OK** をクリックします。

ステップ 6　表示される設定は、次のようになります。入力した情報が正しいことを確認します。



ステップ 7　**Apply** をクリックして、適応型セキュリティ アプライアンスが現在実行中の設定変更を保存します。

これで、プライベート ネットワークおよびパブリック ネットワークのどちらのクライアントも、プライベート ネットワークをセキュアな状態に保ちながら、DMZ Web サーバからのコンテントに対する HTTP 要求を解決できます。

（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、パブリック アドレス 209.165.200.226 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。209.165.200.226 から 10.30.30.30 へのアドレス変換によって、トラフィックが許可されます。変換規則の作成方法の詳細については、P.6-14 の「内部クライアントが DMZ Web サーバと通信するための NAT の設定」を参照してください。

ステップ 8　次回のデバイス起動時に変更が適用されるように、設定変更をスタートアップ設定に保存する場合は、File メニューで **Save** をクリックします。

あるいは、ASDM の終了時に設定変更の保存を要求するプロンプトが表示されます。

設定変更を保存しない場合は、次回のデバイス起動時に以前の設定が有効になります。

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」