シナリオ：DMZ の設定

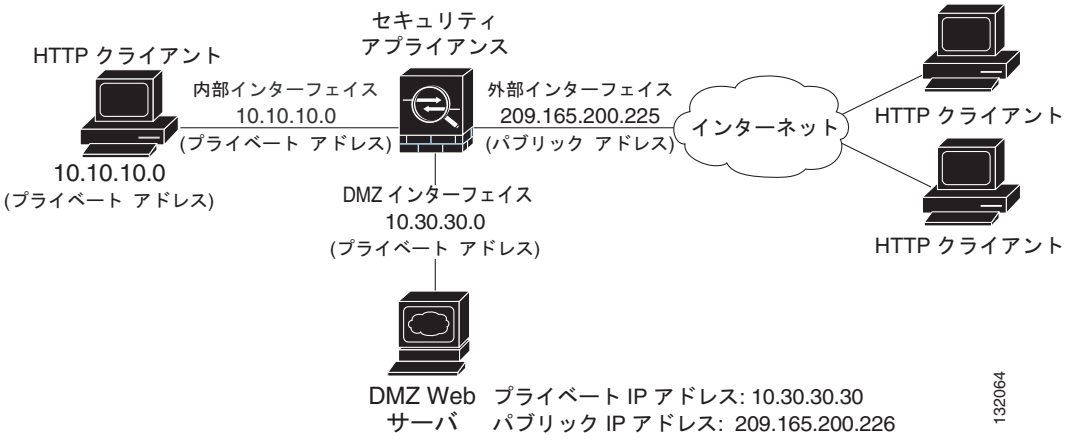
この章では、適応型セキュリティ アプライアンスを使用して非武装地帯（DMZ; demilitarized zone）に置かれたネットワーク リソースを保護するための設定シナリオについて説明します。DMZ とは、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間の中立ゾーンにある区別されたネットワークです。

この章には、次の項があります。

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 実装の典型的なものです。

図 6-1　DMZ の設定シナリオのネットワーク レイアウト



この例のシナリオには、次の性質があります。

- Web サーバは適応型セキュリティ アプライアンスの DMZ インターフェイスにある
- プライベート ネットワーク上の HTTP クライアントは DMZ にある Web サーバにアクセスでき、インターネット上のデバイスとの通信が可能
- インターネット上のクライアントは DMZ Web サーバへの HTTP アクセスが許可され、他のすべてのトラフィックは拒否される
- ネットワークには、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）と、DMZ Web サーバのパブリック IP アドレス（209.165.200.226）という、パブリックに使用可能な 2 つのルーティング可能 IP アドレスがある

図 6-2 に、DMZ Web サーバとインターネットの両方に対してプライベート ネットワークから出される HTTP 要求の発信トラフィック フローを示します。

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

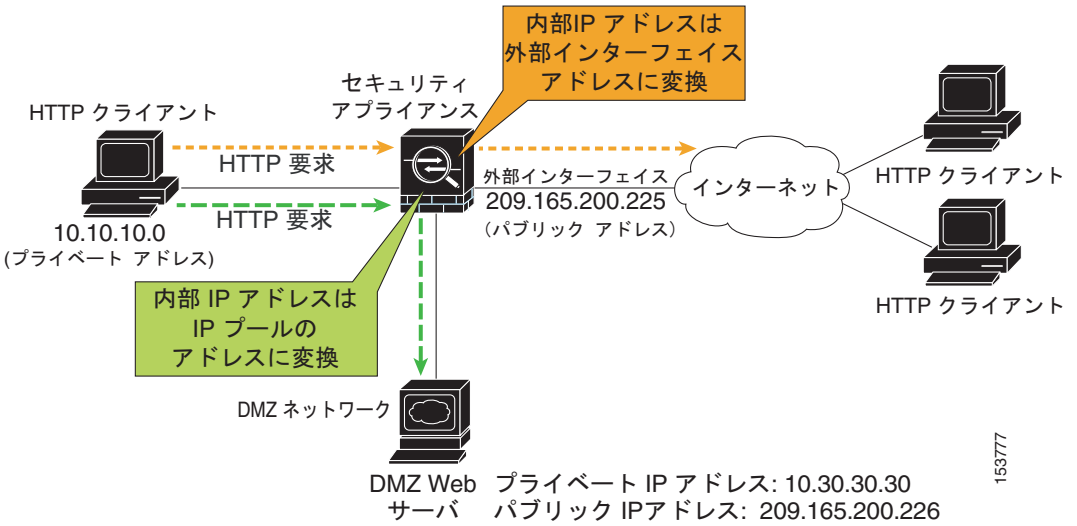


図 6-2 では、DMZ Web サーバとインターネット上のデバイスの両方を宛先として内部クライアントからトラフィックを発信することが適応型セキュリティ アプライアンスによって許可される様子を示します。トラフィックの通過を許可するために、適応型セキュリティ アプライアンスの設定には次のものが含まれます。

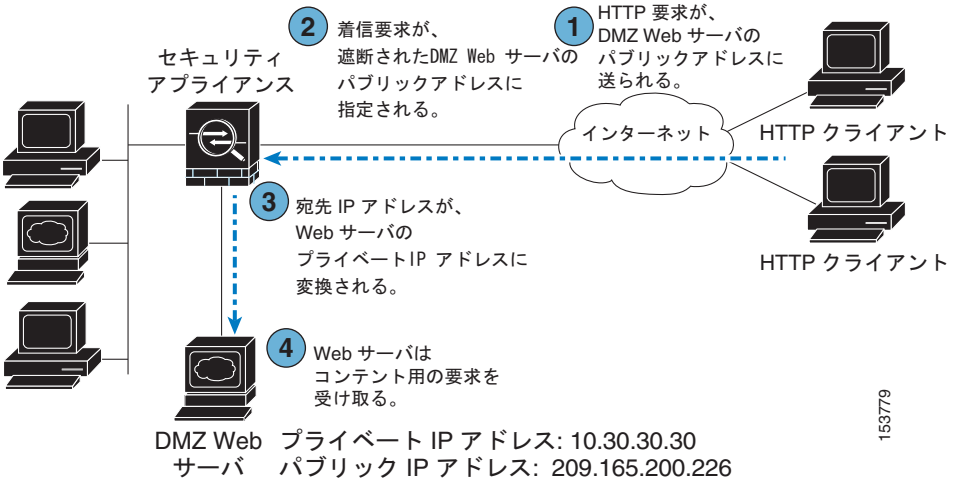
- DMZ Web サーバとインターネット上のデバイスを宛先としたトラフィックを許可するアクセス コントロール規則
- プライベート IP アドレスをプライベート アドレスがインターネットから不可視になるように変換するアドレス変換ルール

  DMZ Web サーバを宛先とするトラフィックには、プライベート IP アドレスは IP プールのアドレスに変換されます。

  インターネットを宛先とするトラフィックには、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送出されると思われます。

図 6-3 に、DMZ Web サーバのパブリック IP アドレスを宛先としてインターネットから発信される HTTP 要求の例を示します。

図 6-3　インターネットからの HTTP トラフィック フローの着信



DMZ Web サーバにアクセスする着信トラフィックを許容するための適応型セキュリティ アプライアンスの設定には次のものが含まれます。

- 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 アドレスに変換するアドレス変換ルール
- DMZ Web サーバを宛先とする HTTP トラフィックの着信を許容するアクセス コントロール規則

この設定を作成するための手順については、この章の以降のページ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

この項では、ASDM を使用して図 6-1 で示した設定シナリオ用に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。手順では、このシナリオに基づいたサンプル パラメータを使用します。

この設定手順では、適応型セキュリティ アプライアンスで、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のインターフェイスをすでに設定していることを前提にしています。適応型セキュリティ アプライアンス用に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。

ここでは、次のトピックについて取り上げます。

- 設定の要件（P.6-6）
- ASDM の設定（P.6-7）
- ネットワーク アドレス変換用の IP プールの作成（P.6-8）
- 内部クライアントが DMZ Web サーバと通信するための NAT を設定する（P.6-14）
- 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 を設定する（P.6-17）
- DMZ Web サーバの外部アイデンティティの設定（P.6-17）
- DMZ Web サーバへのパブリック HTTP アクセスの提供（P.6-20）

次の項では、各手順の実行方法について詳しく説明していきます。

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、次の設定タスクが必要です。

- 内部クライアントで DMZ Web サーバに HTTP アクセスできるようにするために、アドレス変換用の IP アドレスのプールを作成する必要があり、このプールのアドレスを使用するクライアントを識別する必要があります。このタスクを実行するには、次のものを設定する必要があります。
  - DMZ インターフェイスの IP アドレスのプール。このシナリオでは、IP アドレスのプールは 10.30.30.50 ～ 10.30.30.60 です。
  - IP プールからのアドレス割り当てが可能なクライアントを指定する、内部インターフェイス用のダイナミック NAT 変換ルール。
- 内部クライアントがインターネット上の HTTP リソースまたは HTTPS リソースにアクセスできるようにするために、インターネット クライアントの実 IP アドレスを送信元アドレスとして使用できる外部アドレスに変換するためのルールを作成する必要があります。

  このためには、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 PAT 変換ルール（ポート アドレス変換ルール、インターフェイス NAT と呼ばれる場合もある）を設定する必要があります。

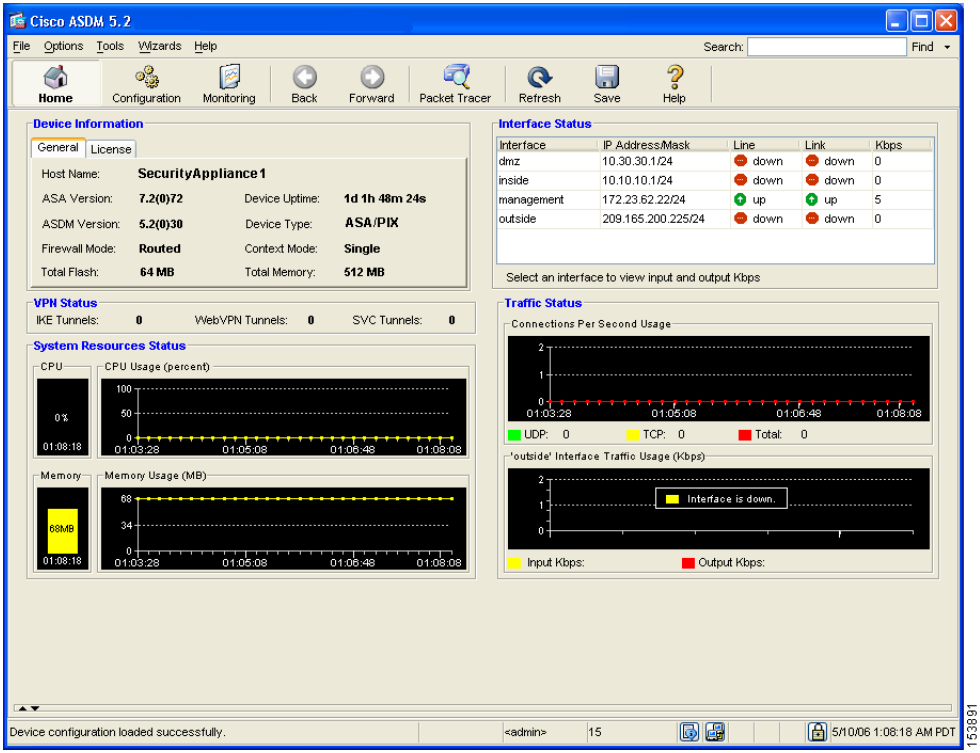
  このシナリオでは、変換される内部アドレスは、プライベート ネットワーク（10.10.10.0）のサブネットのアドレスです。このサブネットのアドレスは、適応型セキュリティ アプライアンスのパブリック アドレス（209.165.200.225）に変換されます。
- 外部クライアントが DMZ Web サーバに HTTP アクセスできるようにするために、DMZ Web サーバの外部アイデンティティと、インターネット上のクライアントから送信される HTTP 要求を許容するアクセス ルールを設定する必要があります。このタスクを実行するには、次のものを設定する必要があります。
  - 静的 NAT ルールを作成します。このルールによって 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）。
  - トラフィックが DMZ Web サーバのパブリック IP アドレスを宛先とする HTTP 要求の場合、インターネットからのアクセスを許容するセキュリティ アクセス規則を作成します。

ASDM の設定

Web ブラウザで ASDM を実行するには、アドレス フィールドに、工場出荷時のデフォルトの 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

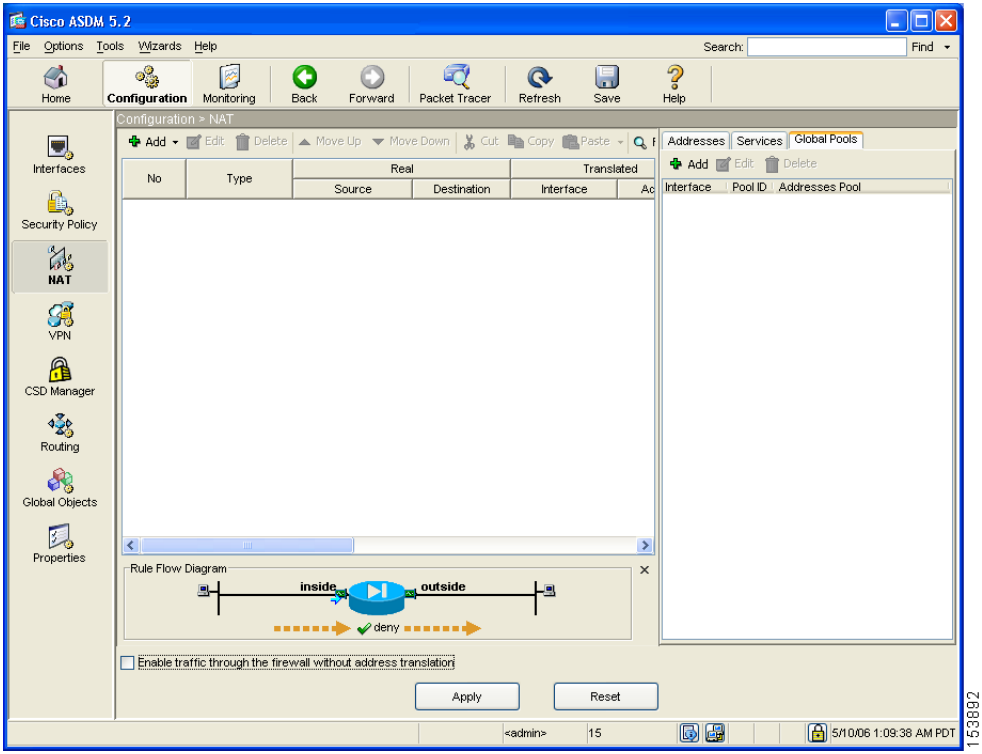
適応型セキュリティ アプライアンスは、ネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）を使用して、内部 IP アドレスが外部に公開されることを防いでいます。ここでは、DMZ インターフェイスと外部インターフェイスがアドレス変換用に使用可能な IP アドレスのプールを作成する方法について説明します。

単一の IP プールに NAT エントリと PAT エントリを両方含めたり、複数のインターフェイスのエントリを含めることができます。

ネットワーク アドレス変換に使用可能な 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。

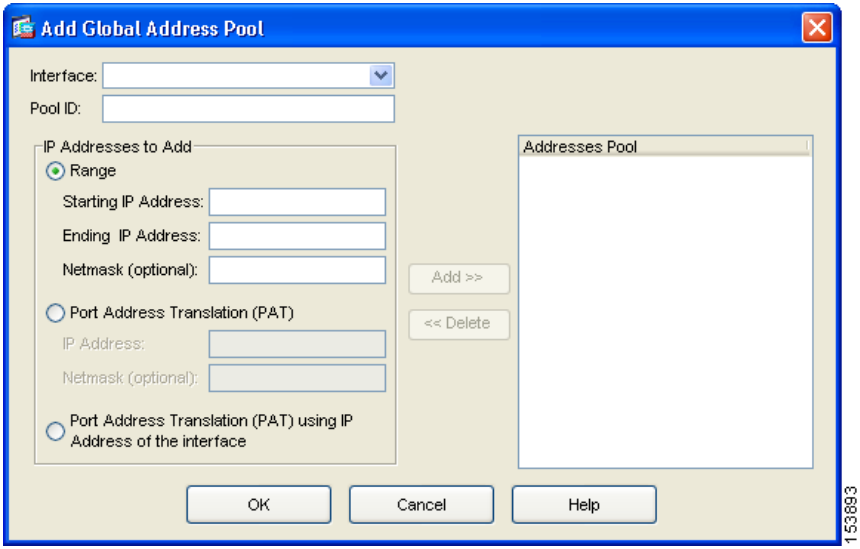


b. 右ペインで、**Global Pools** タブをクリックします。

c. **Add** をクリックして DMZ インターフェイス用のグローバル プールを新規作成します。

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 を選択します。

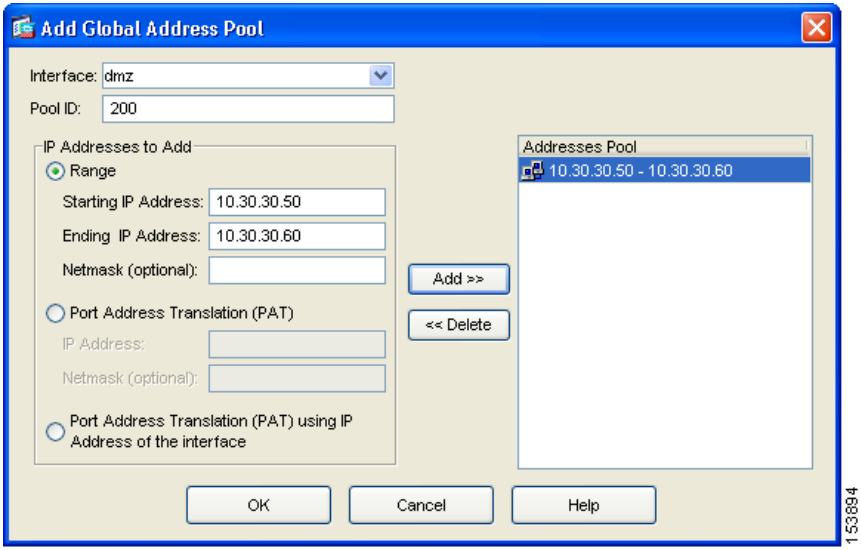
e. 新しい IP プールを作成するには、一意の Pool ID を入力します。このシナリオでは、Pool ID は 200 です。

f. IP Addresses to Add 領域で、DMZ インターフェイスで使用する IP アドレスの範囲を次のように指定します。

- **Range** オプション ボタンをクリックします。
- アドレスの範囲を指定する Starting IP Address と Ending IP Address 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 Netmask 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 Address Pool に追加します。

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



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、内部クライアントが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るように、プライベート IP アドレスを変換する目的で使用します。

このシナリオでは、使用できるパブリック IP アドレスの数が制限されています。次の手順でポート アドレス変換（PAT）を行うことで、多数の内部 IP アドレスが同じパブリック IP アドレスにマッピングできるようにします。

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。

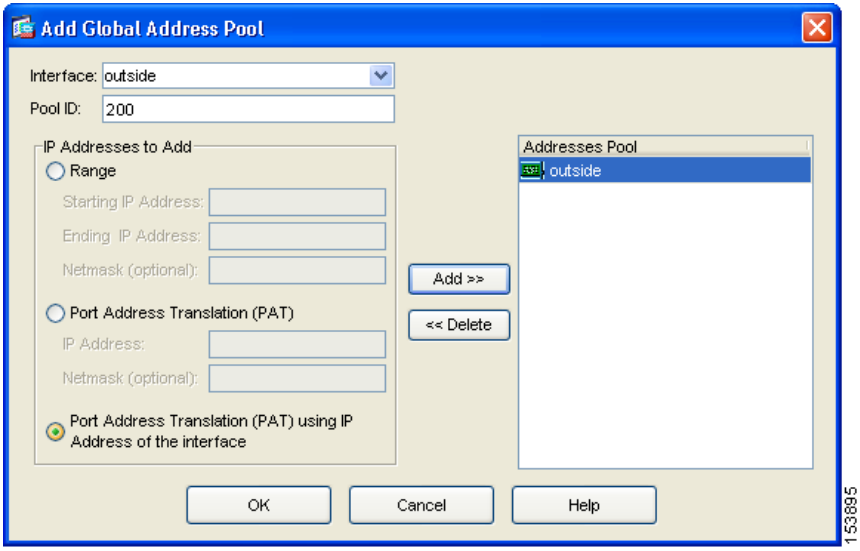
d. outside インターフェイス用の Pool ID を指定します。

DMZ インターフェイスが使用するアドレス プールが含まれる 1 つの IP プール（このシナリオでは Pool ID は 200）に、これら複数のアドレスを追加することができます。

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

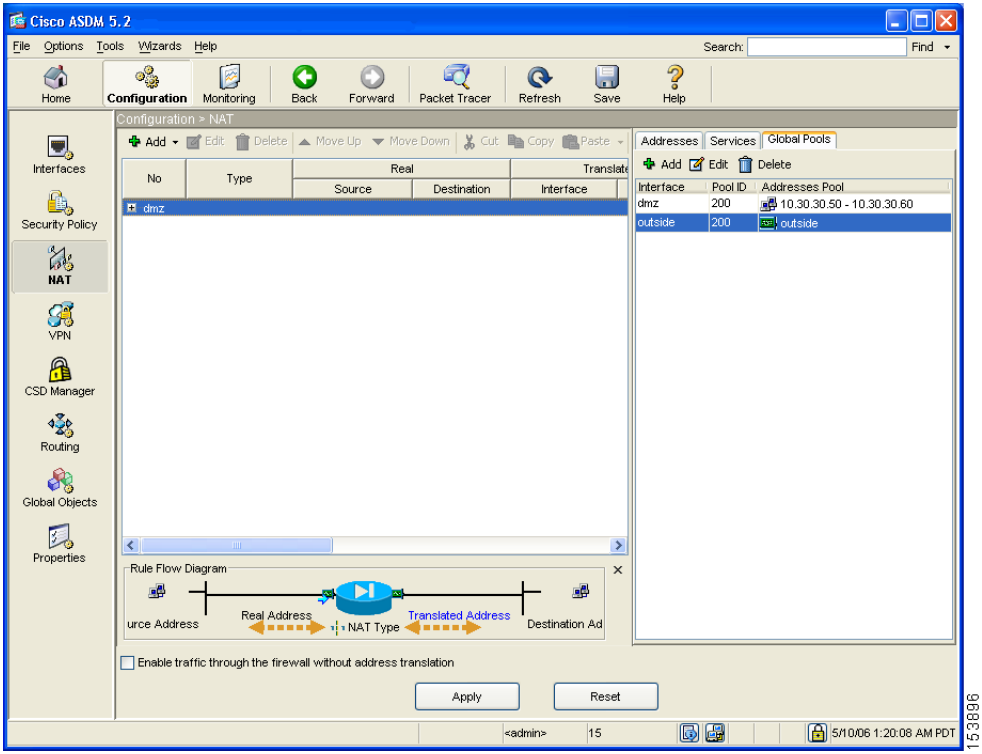
この Port Address Translation（PAT）using the IP address of the interface オプションを選択した場合、内部ネットワークから開始されたすべてのトラフィックは、外部インターフェイスの IP アドレスを使用して適応型セキュリティ アプライアンスを終了します。インターネット上のデバイスにとっては、すべてのトラフィックがこの 1 つの IP アドレスから着信しているように見えます。

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 を設定する

前述した手順では、内部クライアントのプライベート IP アドレスをマスクするために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ました。

この手順では、このプールの IP アドレスと内部クライアントとを関連付けるネットワーク アドレス変換（NAT）ルールを設定して、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。

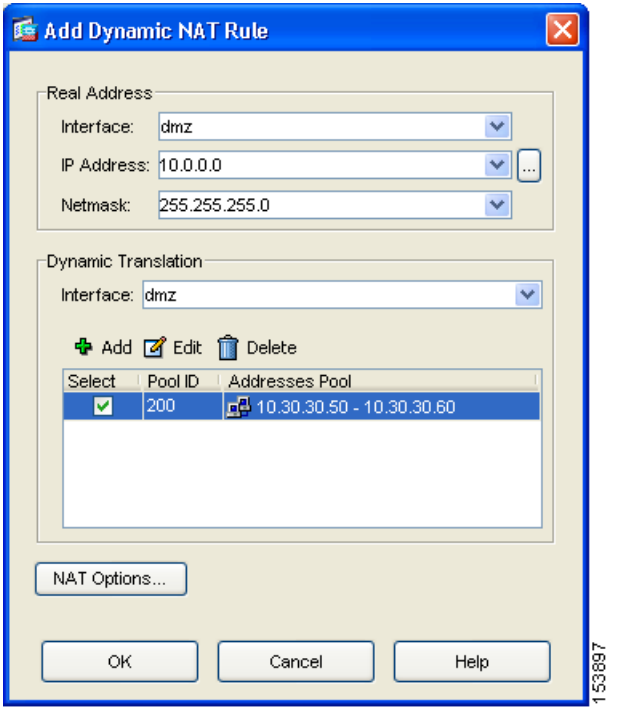
ステップ 4　Real Address 領域で変換する IP アドレスを指定します。このシナリオでは、内部クライアントのアドレス変換はサブネットの IP アドレスに従って行われます。

- **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、Netmask 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 ルールで使用するアドレス プールを指定するには、Global Pool ID の横の **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 プールの ID は 200 です。

  このシナリオでは、使用する予定の IP プールはすでに作成済みです。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 ルールを追加し、Configuration > NAT ウィンドウに戻ります。

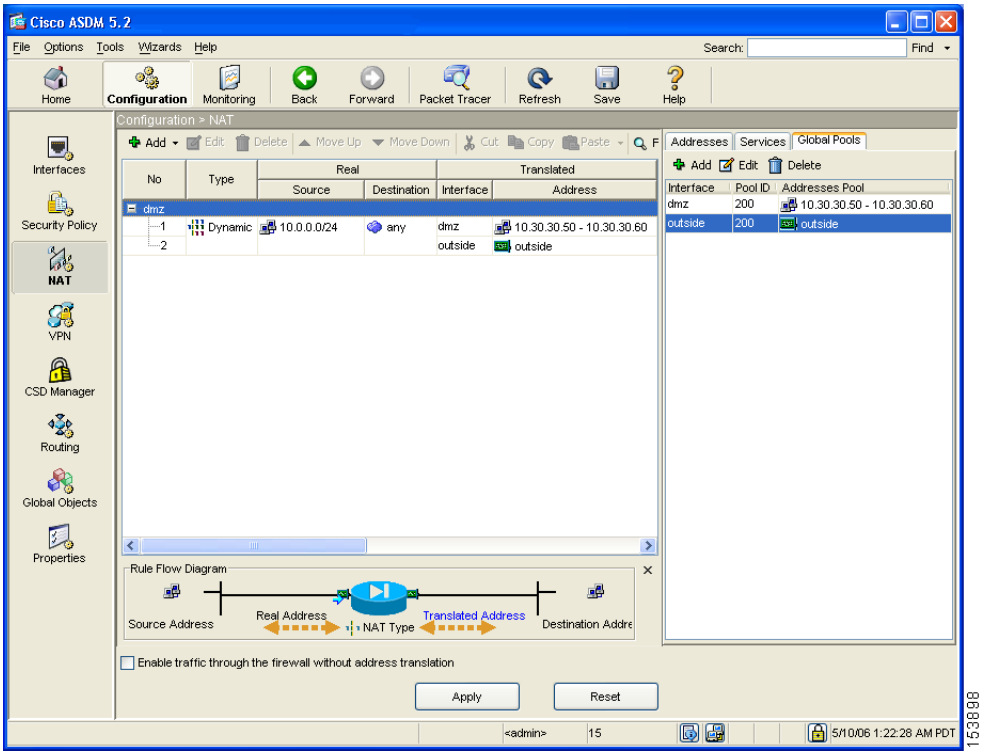
設定画面に変換ルールが予想どおりに表示されることを確認します。

（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 つの変換ルールが作成されていることが分かります。

- 内部クライアントと DMZ Web サーバが通信する場合に使用される、内部インターフェイスと DMZ インターフェイスとの間の変換ルール
- 内部クライアントがインターネットと通信する場合に使用される、内部インターフェイスと外部インターフェイスとの間の変換ルール

変換で使用されるアドレスは両方とも同じ IP プールにあるため、ASDM はこれらの両ルールを作成することができます。

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 を設定する

先ほどの手順では、IP プールの IP アドレスと内部クライアントを関連付けるネットワーク アドレス変換（NAT）ルールを設定して、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しました。

これ以外にも、内部インターフェイスと外部インターフェイスとの間に NAT ルール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多数の設定が必要になります。

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。これは、IP プール（プール ID は 200）に、アドレス変換に必要な両タイプのアドレス、つまり、DMZ インターフェイスで使用される IP アドレスの範囲と、外部インターフェイスで使用される IP アドレスの範囲の 2 種類が含まれているためです。このため、ユーザに代わって ASDM が 2 番目の変換ルールを作成することができます。

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せずに外部の 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。実 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（209.165.200.226）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 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。

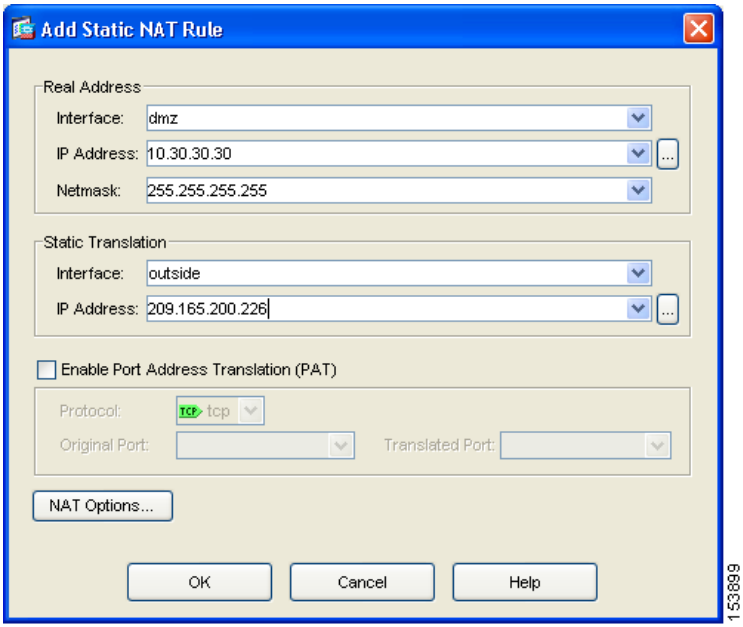
ステップ 3　Add ドロップダウン リストで、Add Static NAT Rule を選択します。Add Static NAT Rule ダイアログボックスが表示されます。

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

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、Web サーバに使用する IP アドレスを次のように指定します。

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

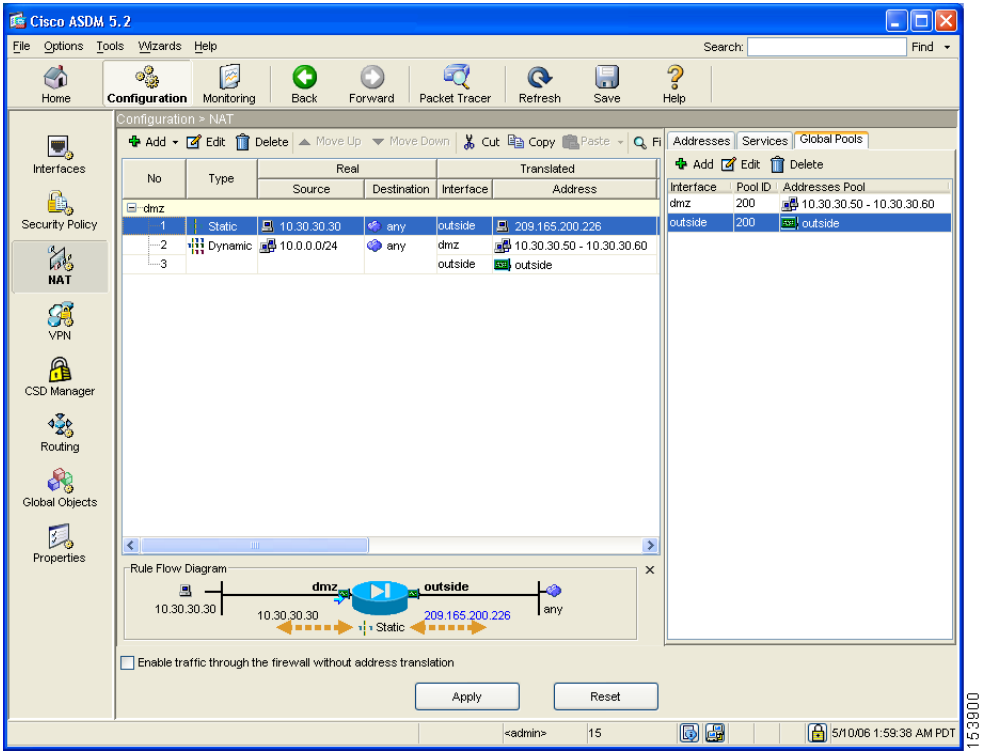
b. IP Address ドロップダウン リストで、DMZ Web サーバのパブリック IP アドレスを選択します。

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** をクリックしてルールを追加し、Address Translation Rules リストに戻ります。

このルールは実 Web サーバの 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プします。

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 のリソースに到達することを許容する必要があります。このアクセス コントロール規則によって、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を指定して、トラフィックが着信と発信のどちらか、トラフィックの発信元と宛先、トラフィック プロトコルの種類、許容すべきサービスなどについて制御します。

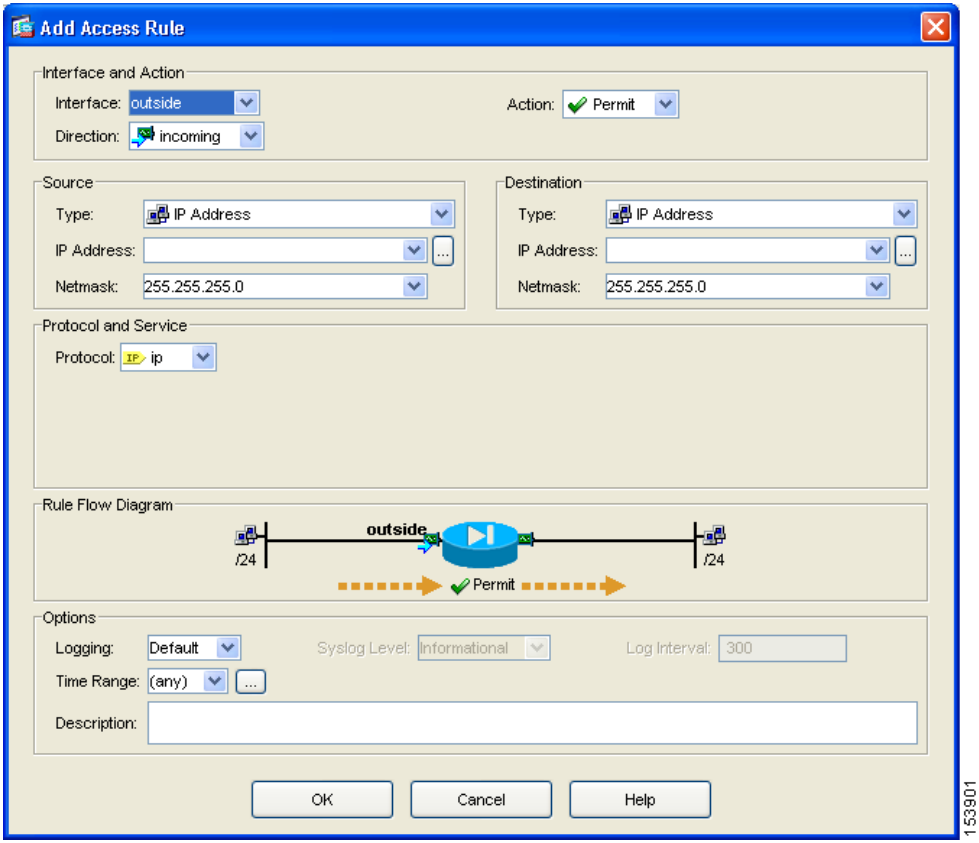
この項では、インターネット上の任意のホストまたはネットワークから発信される HTTP トラフィックの宛先が DMZ ネットワークの Web サーバの場合にこのトラフィックの着信を許容するアクセス規則を作成します。パブリック ネットワークからの他のすべてのトラフィックは拒否されます。

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** タブをクリックしてから、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 をクリックします。
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ネットワークが事前設定済みの場合は、IP Address ドロップダウン リストでその発信元の IP アドレスを選択します。

c. 発信元 IP アドレス用のネットマスクを入力するか、Netmask ドロップダウン リストからいずれかを選択します。

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）。

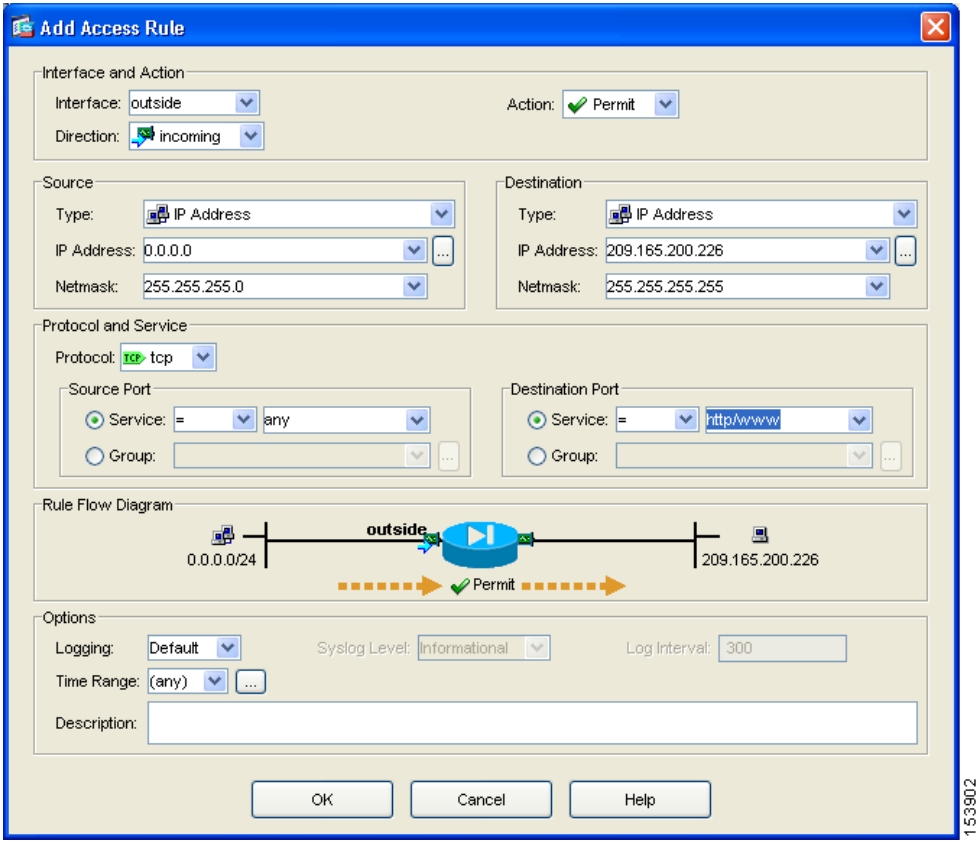
ステップ 5　Protocol and Service 領域で、適応型セキュリティ アプライアンスで許容するトラフィックの種類を指定します。

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 リストから「=」（等号）を選択してから、隣のドロップダウン リストで any を選択します。

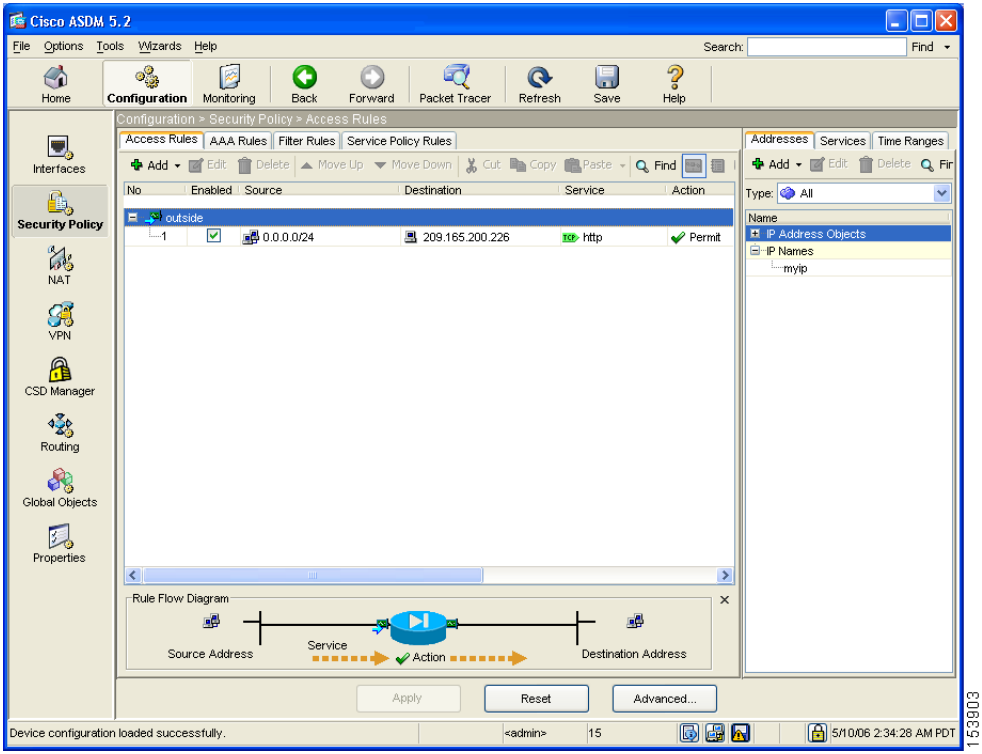
c. Destination Port 領域で、**Service** オプション ボタンをクリックし、Service ドロップダウン リストから「=」（等号）を選択してから、隣のドロップダウン リストで HTTP/WWW を選択します。

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、変更した設定を適応型セキュリティ アプライアンスで現在実行中の設定に保存します。

これで、パブリック ネットワークとプライベート ネットワークの両方のクライアントは、プライベート ネットワークの安全性を維持しながら DMZ Web サーバからのコンテンツに対する HTTP 要求を解決できるようになります。

（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 アドレスの 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。アドレス変換（209.165.200.226 から 10.30.30.30）によって、トラフィックが許可されます。変換ルールの作成の詳細については、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 を設定する」を参照してください。

ステップ 8　設定の変更をスタートアップ設定に保存して、デバイスを次回に起動したときにこの変更が適用されるようにする場合は、File メニューの **Save** をクリックします。

あるいは、ASDM の終了時に、設定の変更を保存するかどうか確認を求めるメッセージが表示されます。

設定の変更を保存しないと、次回にデバイスを起動したときに、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*

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」