CHAPTER 8

シナリオ：DMZ の設定

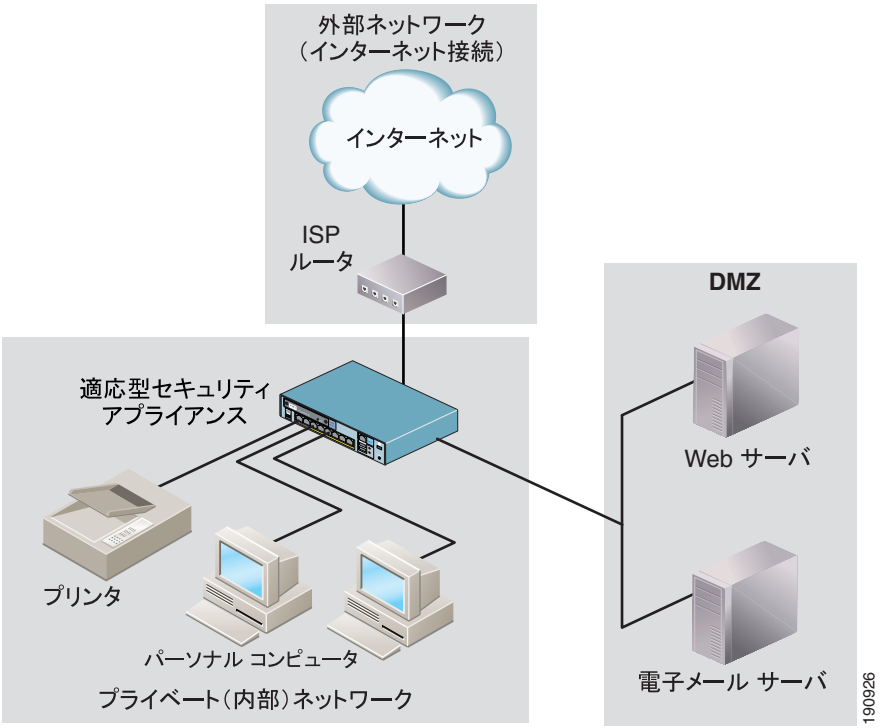
非武装地帯（DMZ）とは、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間の中立ゾーンにある区別されたネットワークです。

この章は、次の項で構成されています。

DMZ 設定用の基本ネットワーク レイアウト

図 8-1 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 実装の代表的なものです。この配置では、Web サーバは DMZ インターフェイス上にあり、HTTP クライアントは内部ネットワークからも外部ネットワークからもこの Web サーバにセキュアにアクセスできます。

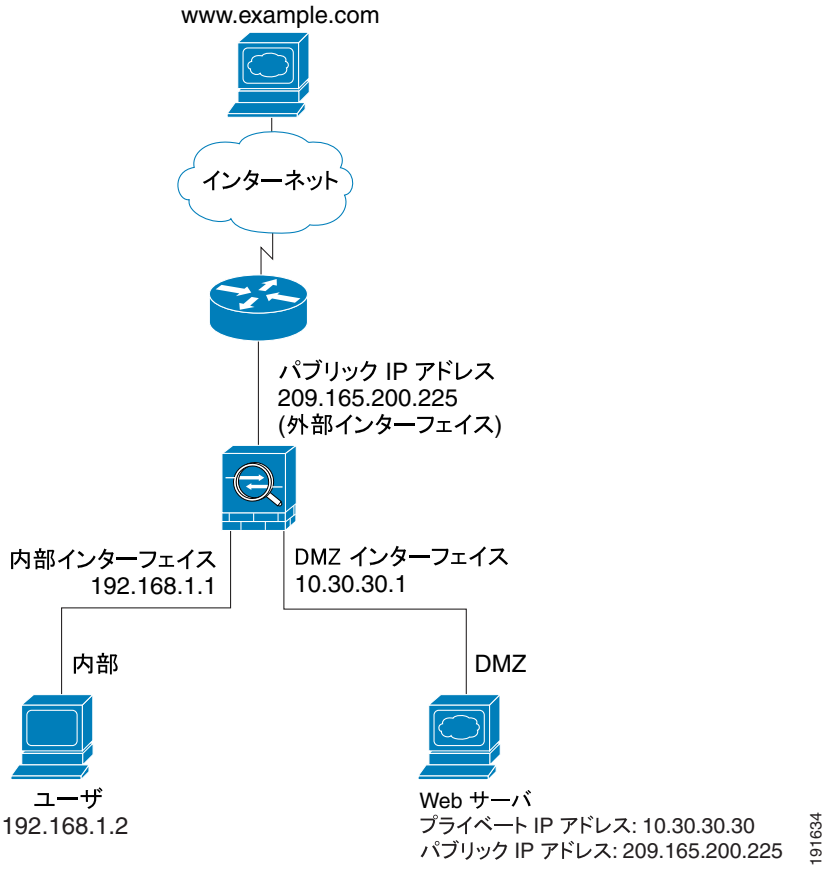
図 8-1　　DMZ を使用したプライベート ネットワーク



DMZ ネットワーク トポロジの例

この章では、適応型セキュリティ アプライアンスの DMZ の配置を設定する方法について説明します（図 8-2 を参照してください）。

図 8-2　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、インターネット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。
- ネットワークには、パブリックに使用可能な IP アドレス、つまり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）があります。このパブリック アドレスは、適応型セキュリティ アプライアンスおよび DMZ Web サーバで共有されます。

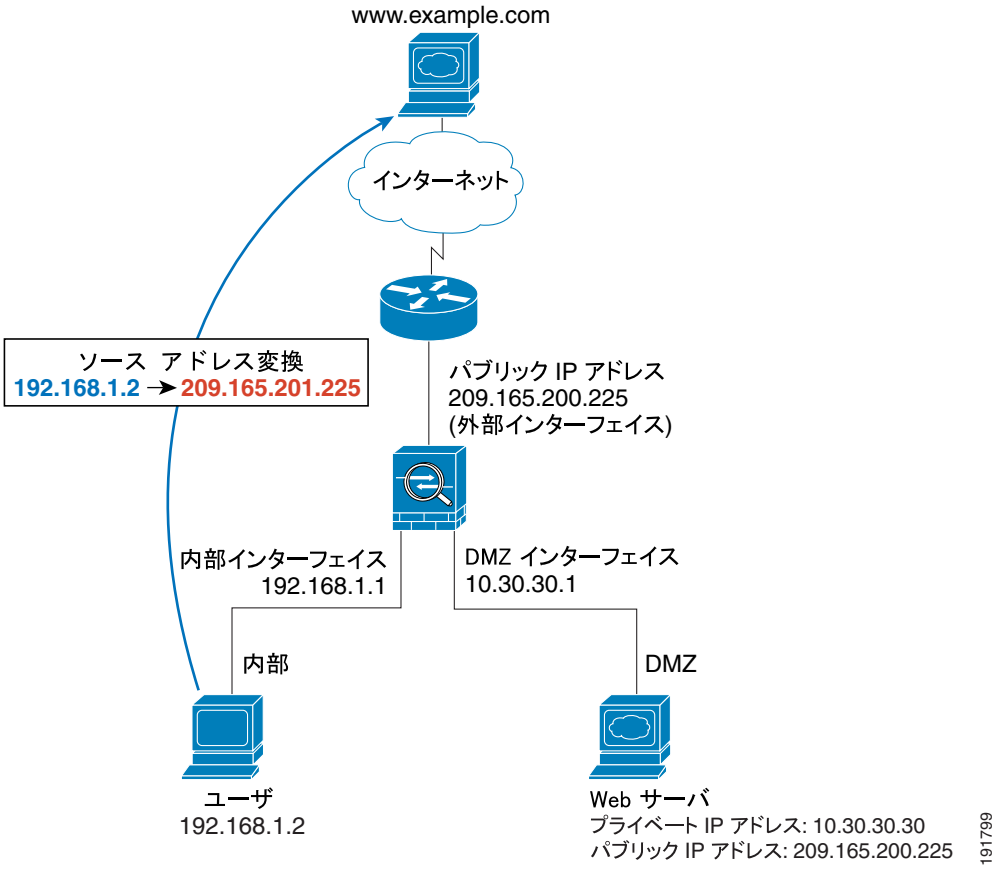
この項では、次のトピックについて取り上げます。

- インターネット上の Web サーバにアクセスする内部ユーザ（P.8-5）
- DMZ Web サーバにアクセスするインターネット ユーザ（P.8-7）
- DMZ Web サーバにアクセスする内部ユーザ（P.8-9）

インターネット上の Web サーバにアクセスする内部ユーザ

図 8-3 は、内部ユーザがインターネット上の Web サーバに HTTP ページを要求したときの、適応型セキュリティ アプライアンスを通るトラフィック フローを示しています。

図 8-3　インターネット上の Web サーバにアクセスする内部ユーザ



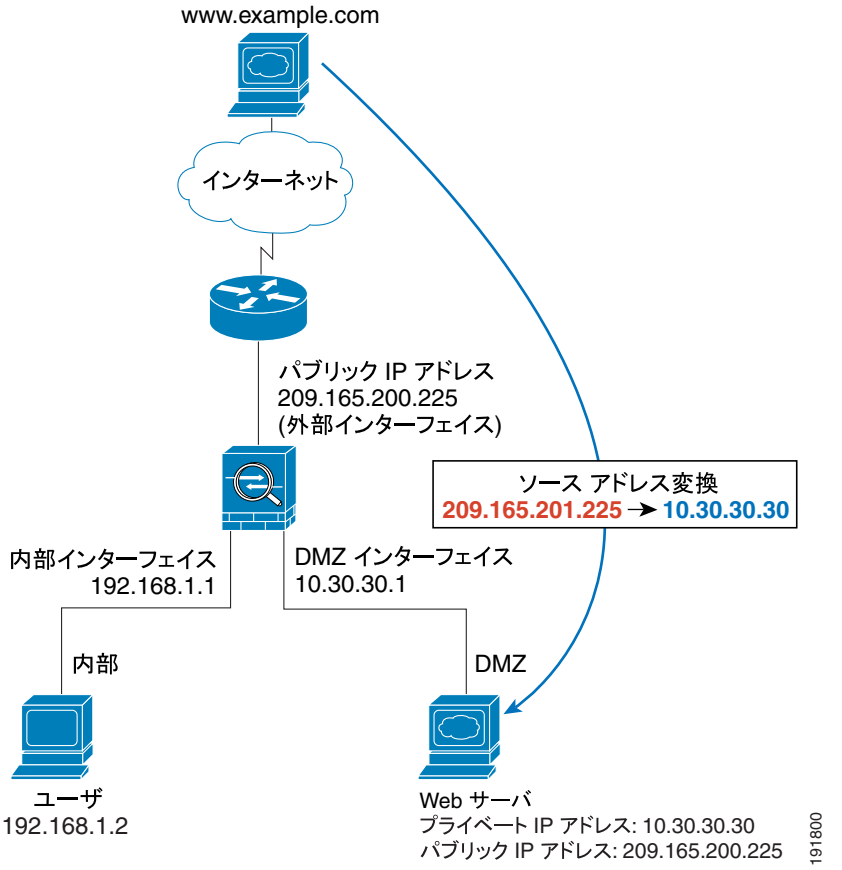
内部ユーザがインターネット上の Web サーバに HTTP ページを要求すると、データは次のように適応型セキュリティ アプライアンスを通じて移動します。

1. 内部ネットワーク上のユーザが www.example.com に Web ページを要求します。
2. 適応型セキュリティ　アプライアンスはパケットを受信します。これは新しいセッションのため、このパケットが許可されていることを確認します。
3. 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）を行い、ローカルの送信元アドレス（192.168.1.2）を外部インターフェイスのパブリック アドレス（209.165.200.225）に変換します。
4. 適応型セキュリティ　アプライアンスはセッションが確立されたことを記録し、外部インターフェイスからこのパケットを転送します。
5. www.example.com が要求に応答すると、パケットは確立されたセッションを使用して適応型セキュリティ アプライアンスを通過します。
6. 適応型セキュリティ アプライアンスは NAT を実行し、パブリックの宛先アドレスをローカル ユーザ アドレス（192.168.1.2）に変換します。
7. 適応型セキュリティ アプライアンスはパケットを内部ユーザに転送します。

DMZ Web サーバにアクセスするインターネット ユーザ

図 8-4 は、インターネット上のユーザが DMZ Web サーバに Web ページを要求したときの、適応型セキュリティ アプライアンスを通るトラフィック フローを示しています。

図 8-4　DMZ Web サーバにアクセスする外部ユーザ



インターネット上のユーザが DMZ Web サーバに HTTP ページを要求すると、トラフィックは次のように適応型セキュリティ アプライアンスを通過します。

1. 外部ネットワーク上のユーザは、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（外部インターフェイスの IP アドレスである 209.165.200.225）を使用して、DMZ Web サーバに Web ページを要求します。
2. 適応型セキュリティ　アプライアンスはパケットを受信します。これは新しいセッションのため、このパケットが許可されていることを確認します。
3. 適応型セキュリティ アプライアンスは、宛先アドレスを DMZ Web サーバのローカル アドレス（10.30.30.30）に変換し、DMZ インターフェイスを通じてパケットを転送します。
4. DMZ Web サーバが要求に応答すると、適応型セキュリティ アプライアンスは、ローカルの送信元アドレスを DMZ Web サーバのパブリック アドレス（209.165.200.225）に変換します。
5. 適応型セキュリティ アプライアンスはパケットを外部ユーザに転送します。

DMZ Web サーバにアクセスする内部ユーザ

図 8-5 は、DMZ Web サーバにアクセスするユーザを示しています。

図 8-5　DMZ 上の Web サーバにアクセスする内部ユーザ

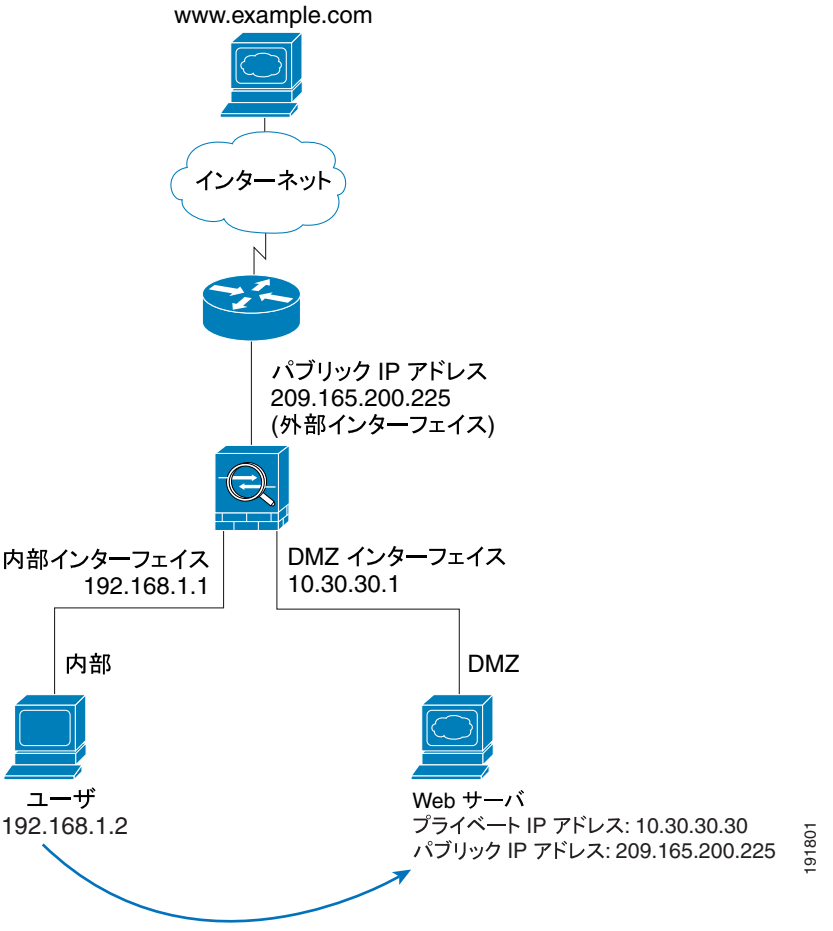


図 8-5 で、適応型セキュリティ アプライアンスは、内部クライアントから発信される DMZ Web サーバ宛の HTTP トラフィックを許可します。内部ネットワークには DNS サーバが存在しないため、内部クライアントの DMZ Web サーバに対する要求は、次のように処理されます。

1. 検索要求は ISP の DNS サーバに送信されます。DMZ Web サーバのパブリック IP アドレスがクライアントに返されます。
2. 内部クライアントは、DMZ Web サーバの IP アドレスに Web ページを要求します。適応型セキュリティ アプライアンスは、内部インターフェイス上でこの要求を受信します。
3. 適応型セキュリティ アプライアンス は DMZ Web サーバの IP アドレスを実アドレス（209.165.200.225 -> 10.30.30.30）に変換し、DMZ インターフェイスから Web サーバに要求を転送します。
4. DMZ Web サーバが要求に応答すると、適応型セキュリティ アプライアンスは DMZ インターフェイス上でデータを受信し、内部インターフェイスからユーザにこのデータを転送します。

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 配置用の適応型セキュリティ アプライアンスの設定

この章では、ASDM を使用して、図 8-2 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、外部インターフェイス、および DMZ 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 7 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。

ここからは、この設定を実装するための手順について説明します。

設定の要件

適応型セキュリティ アプライアンスのこの DMZ 配置には、次の設定規則が必要です。

目的	作成する規則
内部クライアントがインターネット上の Web サーバに情報を要求する	適応型セキュリティ アプライアンスのデフォルト設定では、内部クライアントがインターネット上のデバイスにアクセスすることが許可されています。追加設定は必要ありません。
内部クライアントが DMZ Web サーバに情報を要求する	• DMZ Web サーバの実 IP アドレスをパブリック IP アドレス（10.10.10.30 から 209.165.200.225）に変換する、DMZ および内部インターフェイス間の NAT 規則。 • 内部クライアント ネットワークの実アドレスを変換する、内部および DMZ インターフェイス間の NAT 規則。このシナリオでは、内部ネットワークの実 IP アドレスは自分自身に「変換」されます。つまり、内部クライアントが DMZ Web サーバと通信を行うとき、内部ネットワークの実 IP アドレスが使用されます（10.10.10.0 から 10.10.10.0 に変換）。
外部クライアントが DMZ Web サーバに情報を要求する	• DMZ Web サーバのパブリック IP アドレスをプライベート IP アドレス（209.165.200.225 から 10.10.10.30 に）変換する、外部および DMZ インターフェイス間のアドレス変換規則。 • 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）。

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 内のサーバ用に使用されるパブリック 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、このパブリック IP アドレスを使用して DMZ 内のサーバにアクセスします）。
- 発信トラフィックの内部 IP アドレスの代わりになるクライアント IP アドレス（このシナリオでは、外部インターフェイスの IP アドレス）。IP アドレスが公開されないようにするため、発信クライアントの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。

ASDM の起動

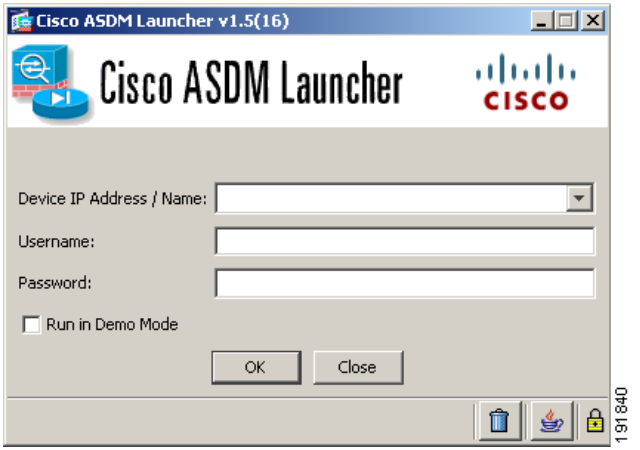
この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。



ステップ 2　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 3　Username および Password フィールドはブランクのままにします。

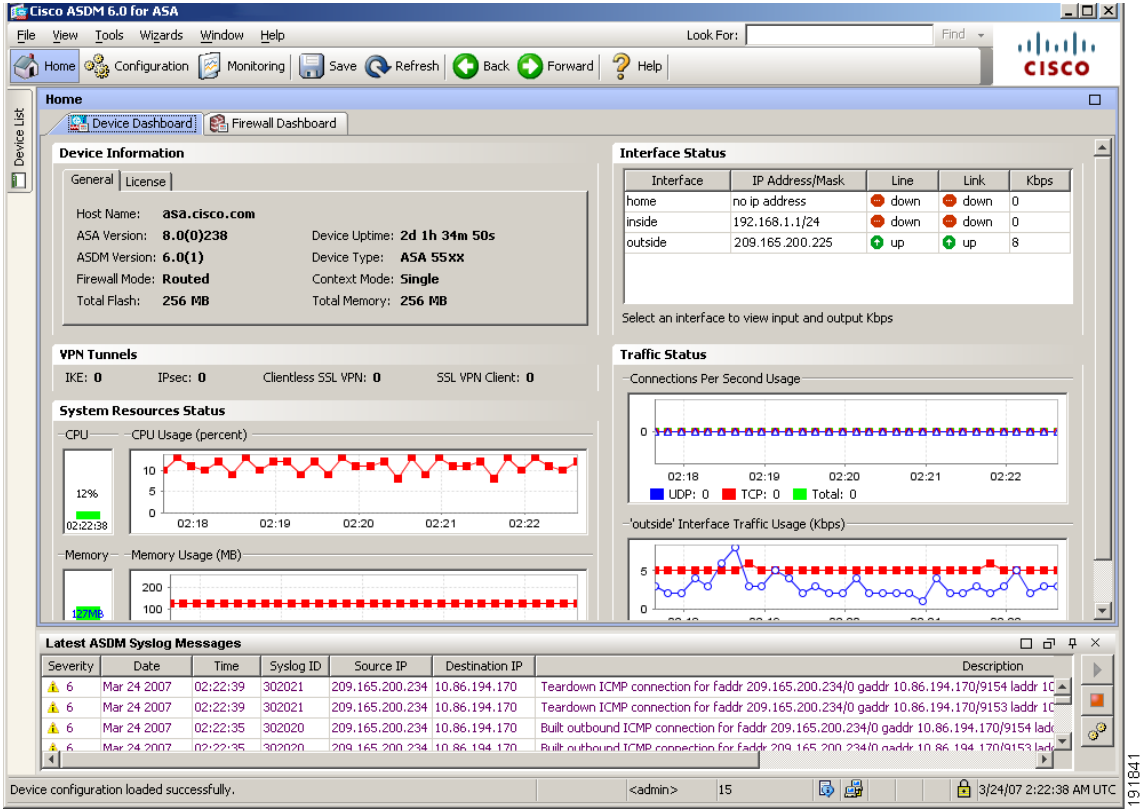
（注）　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes**　をクリックします。

ASA は更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

ASDM のメイン ウィンドウが表示されます。



内部クライアントによるインターネット上のデバイスとの通信の許可

内部クライアントがインターネット上のデバイスにコンテンツを要求できるようにするため、適応型セキュリティ アプライアンスは、内部クライアントの実 IP アドレスを外部インターフェイスの外部アドレス（つまり、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）に変換します。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。

適応型セキュリティ アプライアンスでは、必要なアドレス変換規則がデフォルトで設定されています。内部インターフェイスの IP アドレスを変更しない限り、内部クライアントによるインターネットへのアクセスを許可する設定を行う必要はありません。

内部クライアントによる DMZ Web サーバとの通信の許可

この手順では、内部クライアントが DMZ 内の Web サーバとセキュアに通信できるように、適応型セキュリティ アプライアンスを設定します。これを行うには、次の 2 つの規則を設定する必要があります。

- DMZ Web サーバの実 IP アドレスをパブリック IP アドレス（10.30.30.30 から 209.165.200.225）に変換する、DMZ および内部インターフェイス間の NAT 規則。
- DMZ Web サーバのパブリック IP アドレスを実 IP アドレス（209.165.200.225 から 10.30.30.30）に戻す、内部および DMZ インターフェイス間の NAT 規則。

  内部クライアントが DNS 検索要求を送信すると、DNS サーバは DMZ Web サーバのパブリック IP アドレスを返すため、この規則が必要になります。

（注） 内部ネットワーク上に DNS サーバが存在しないため、DNS 要求は適応型セキュリティ アプライアンスを出て、インターネット上の DNS サーバによって解決される必要があります。

この項では、次のトピックについて取り上げます。

- 内部および DMZ インターフェイス間の内部クライアントの IP アドレス変換（P.8-17）
- Web サーバのパブリック アドレスから実アドレスへの変換（P.8-21）

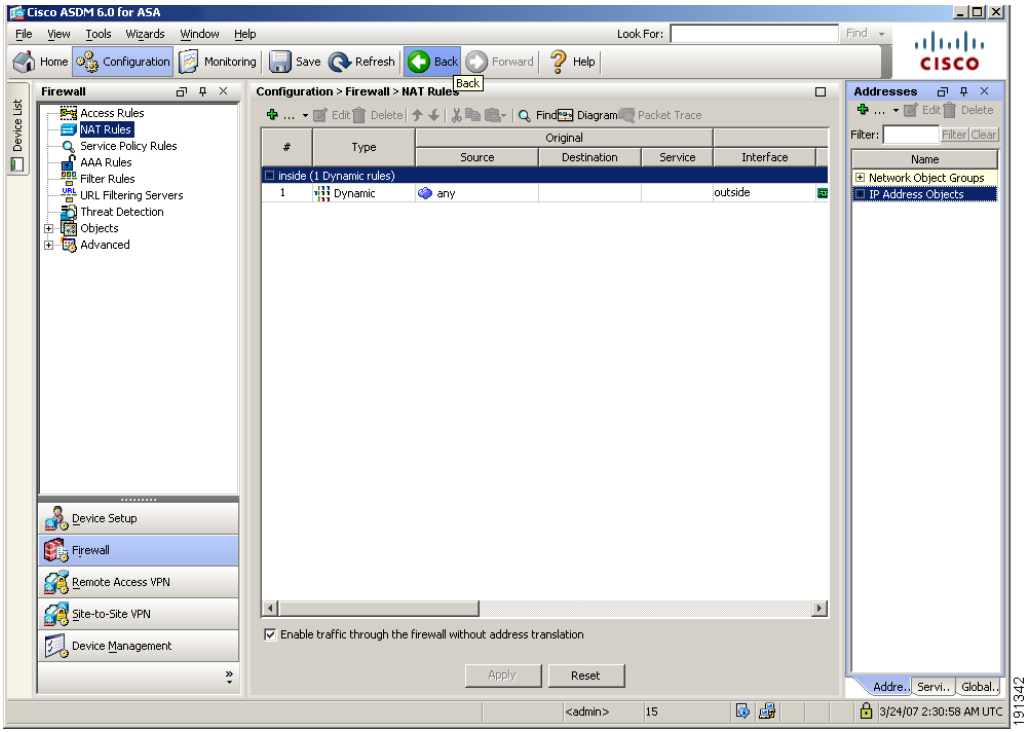
内部および DMZ インターフェイス間の内部クライアントの IP アドレス変換

内部インターフェイスおよび DMZ インターフェイス間で内部クライアントの IP アドレスを変換する NAT 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 のメイン ウィンドウで、**Configuration** ツールをクリックします。

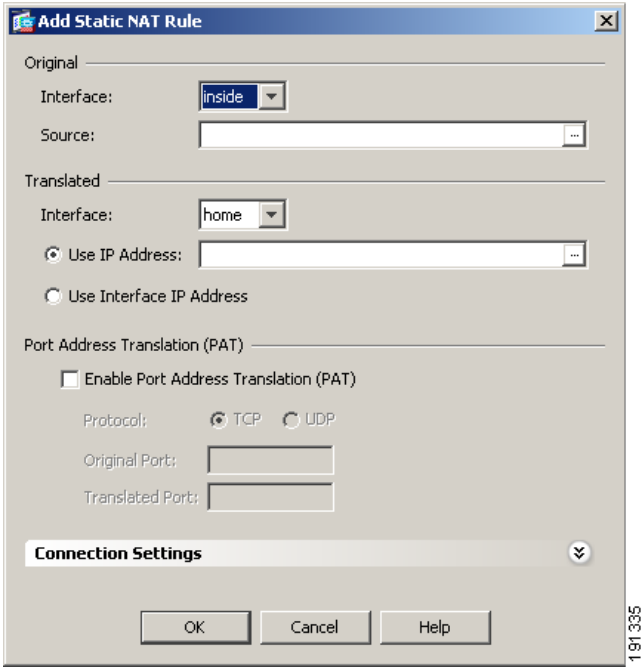
ステップ 2　ASDM ウィンドウの左側にある Device List 領域で、Firewall をクリックします。

ステップ 3　ASDM ウィンドウの左側にある Firewall ペインで、NAT Rules をクリックします。



ステップ 4　緑色のプラス記号（+）のアイコンをクリックし、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 5　Original 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、10.10.10.0 サブネット全体に対して実行されます。

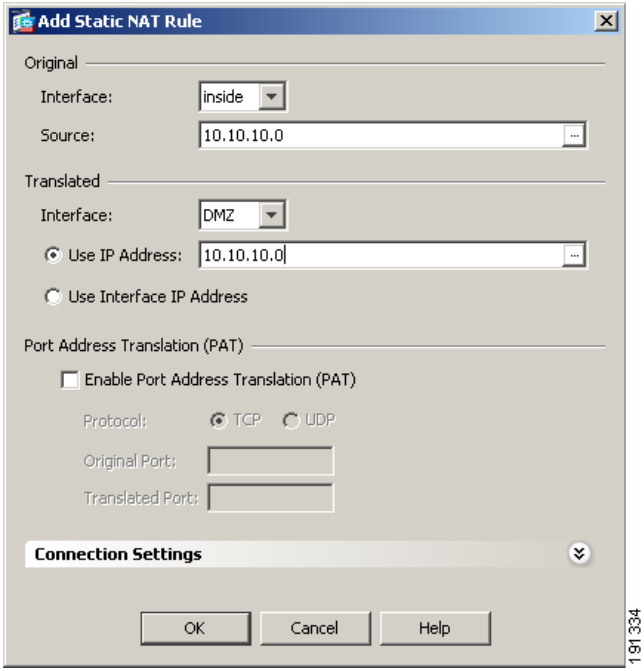
a.　Interface ドロップダウン リストで、inside インターフェイスを選択します。

b.　Source フィールドに、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。

ステップ 6　Translated 領域で、次の手順を実行します。

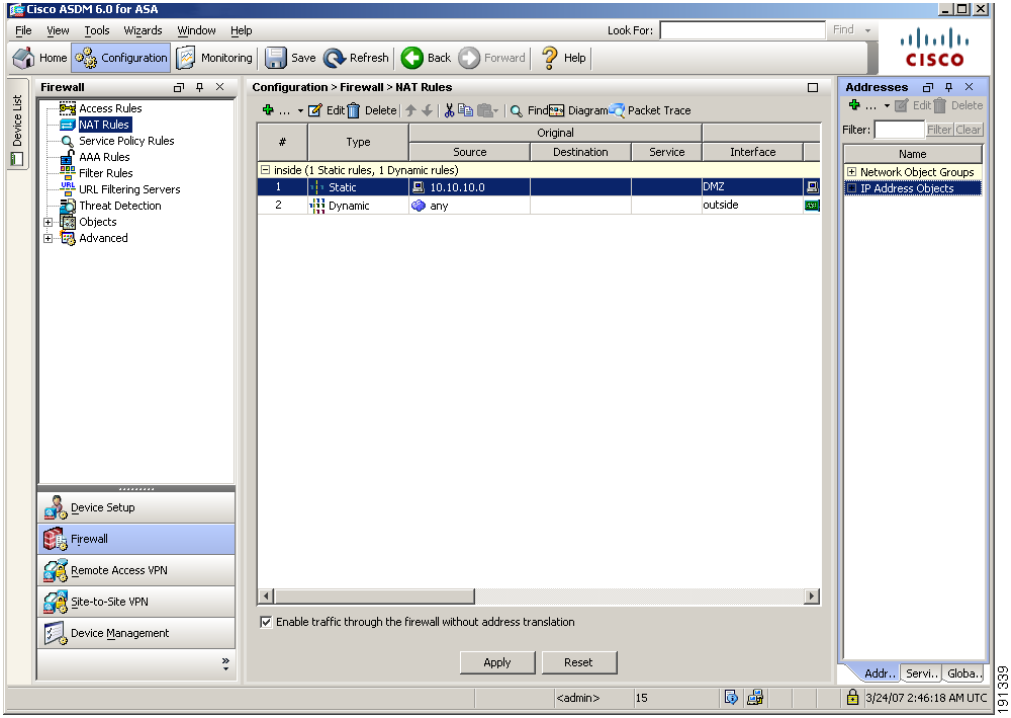
a. Interface ドロップダウン リストで、DMZ インターフェイスを選択します。

b. IP Address フィールドに、内部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. **OK** をクリックして Static NAT Rule を追加し、Configuration > NAT ペインに戻ります。

設定ペインで、変換規則が予想どおりに表示されることを確認します。規則は次のように表示されます。



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。

Web サーバのパブリック アドレスから実アドレスへの変換

Web サーバのパブリック IP アドレスを実 IP アドレスに変換する NAT 規則を設定するには、次の手順を実行します。

ステップ 1　Configuration > Firewall > NAT Rules 画面で、緑色の +（プラス記号）のアイコンをクリックし、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 2　Original 領域で、次の手順を実行します。

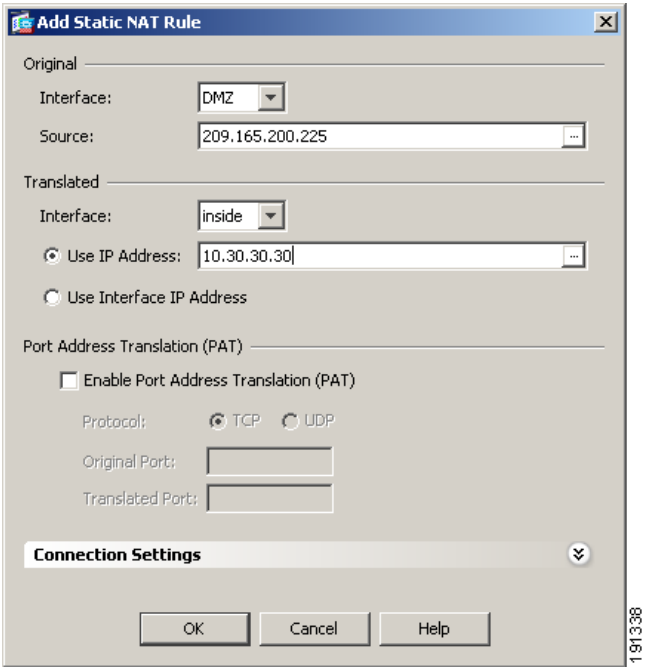
a. Interface ドロップダウン リストで、DMZ を選択します。

b. Source フィールドで、DMZ Web サーバのパブリック アドレスを入力するか、または IP Address ドロップダウン リストから選択します。このシナリオでは、IP アドレスは 209.165.200.225 です。

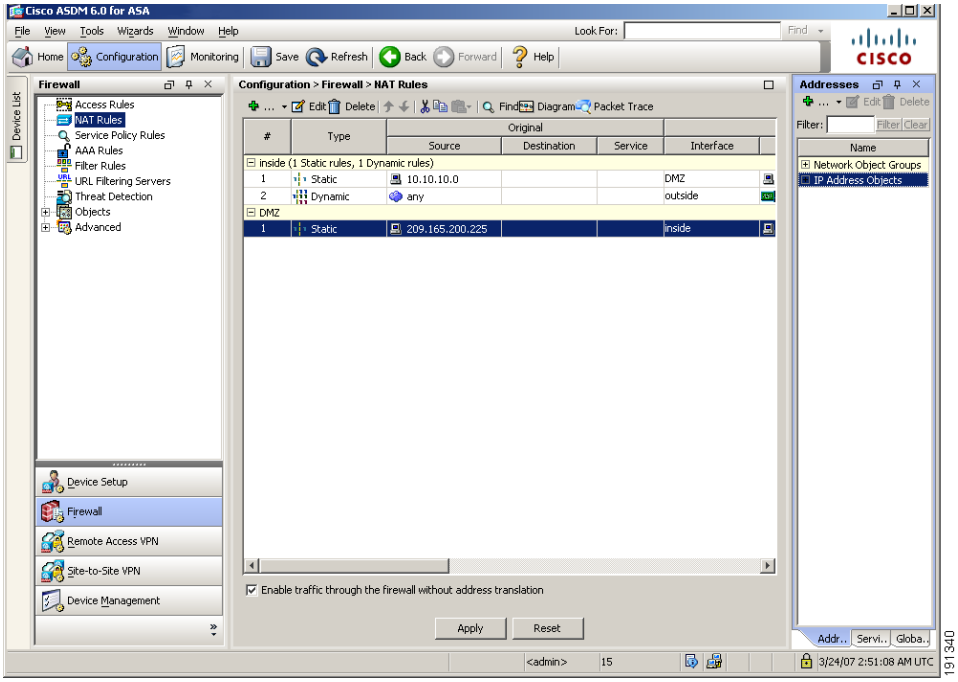
ステップ 3　Translated 領域で、次の手順を実行します。

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

b. DMZ Web サーバの実アドレスを入力するか、または IP Address ドロップダウン リストから選択します。このシナリオでは、IP アドレスは 10.30.30.30 です。


Add Static NAT Rule
Original
Interface:
DMZ
Source:
209.165.200.225
Translated
Interface:
inside
Use IP Address:
10.30.30.30
Use Interface IP Address
Port Address Translation (PAT)
Enable Port Address Translation (PAT)
Protocol:
TCP
UDP
Original Port:
Translated Port:
Connection Settings
OK
Cancel
Help
191338

ステップ 4　**OK** をクリックして、Configuration > NAT ペインに戻ります。表示される設定は、次のようになります。



ステップ 5　**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 アクセス用のスタティック PAT の設定（ポート転送）

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、外部 HTTP クライアントが適応型セキュリティ アプライアンスを意識せずに Web サーバにアクセスできるようにする必要があります。このシナリオでは、DMZ Web サーバは、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）とパブリック IP アドレスを共有しています。

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（209,165,200,225）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　Configuration > Firewall > NAT Rules ペインで、Add ドロップダウン リストから 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 2　Original 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。

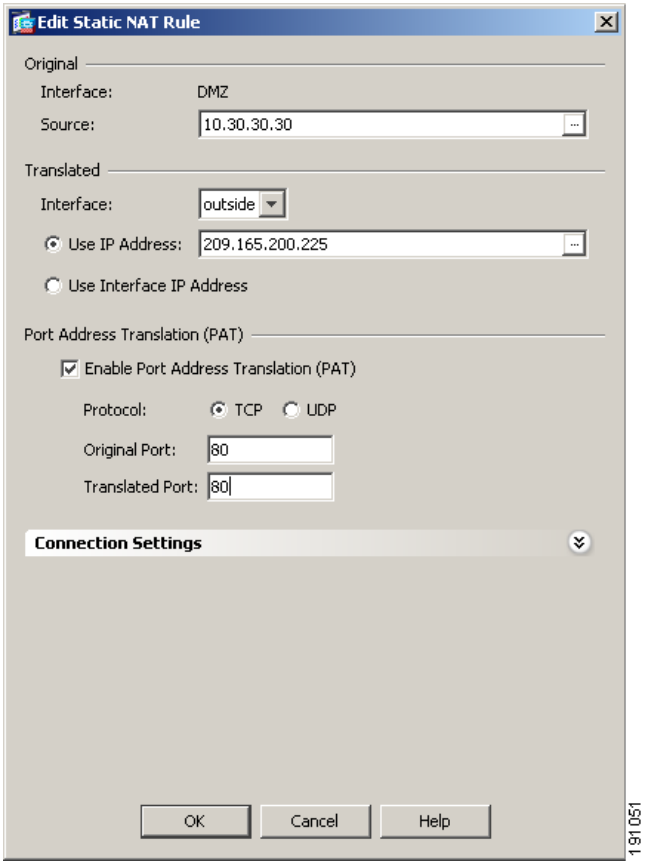
a. Interface ドロップダウン リストで、DMZ インターフェイスを選択します。

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。

ステップ 3　Translated 領域で、Web サーバに使用されるパブリック 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 を選択します。

b. Interface IP オプション ボタンをクリックします。これが指定されたインターフェイス（この場合は外部インターフェイス）の IP アドレスになります。



ステップ 4　ポート アドレス変換を設定します。

パブリック IP アドレスは 1 つしかないため、ポート アドレス変換を使用して、DMZ Web サーバの IP アドレスを、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（外部インターフェイスの IP アドレス）に変換する必要があります。ポート アドレス変換を設定するには、次の手順を実行します。

a.　**Enable Port Address Translation** チェックボックスをオンにします。

b.　TCP Protocol オプション ボタンをクリックします。

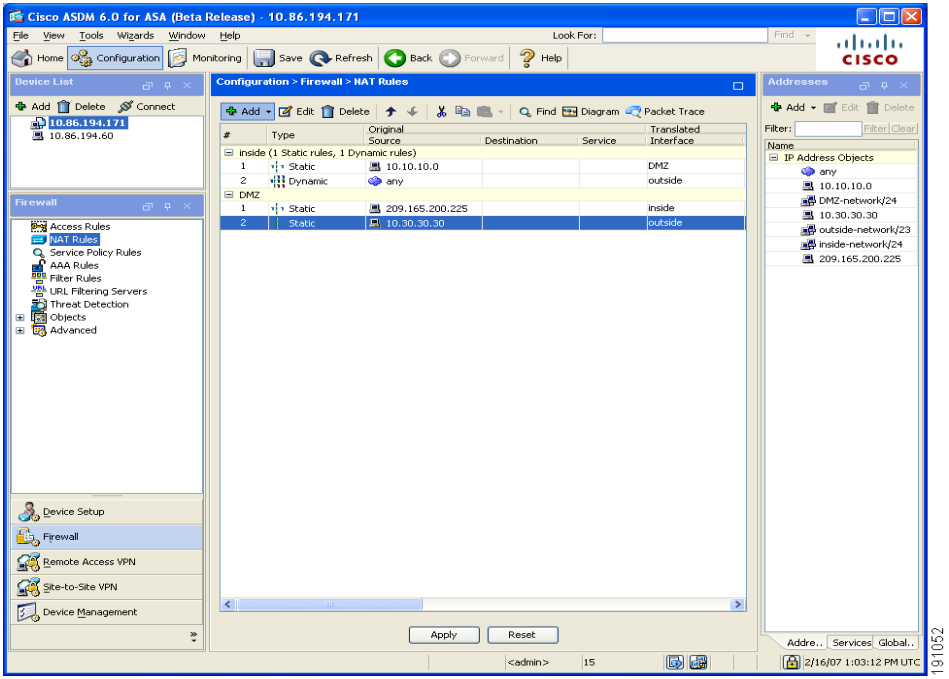
c. Original Port フィールドに 80 を入力します。

d. Translated Port フィールドに 80 を入力します。

e. **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（209,165,200,225）にスタティックにマッピングします。

ステップ 5　規則が予想どおりに作成されたことを確認します。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。

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。インターネットからの着信トラフィックが DMZ Web サーバにアクセスすることを許可するには、DMZ Web サーバ宛の着信 HTTP トラフィックを許可するアクセス コントロールを設定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であること、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 のメイン 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.** Firewall ペインで、**Access Rules** をクリックします。
- **c.** 緑色のプラス記号のアイコンをクリックし、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　Add Access Rule ダイアログボックスで、次の手順を実行します。

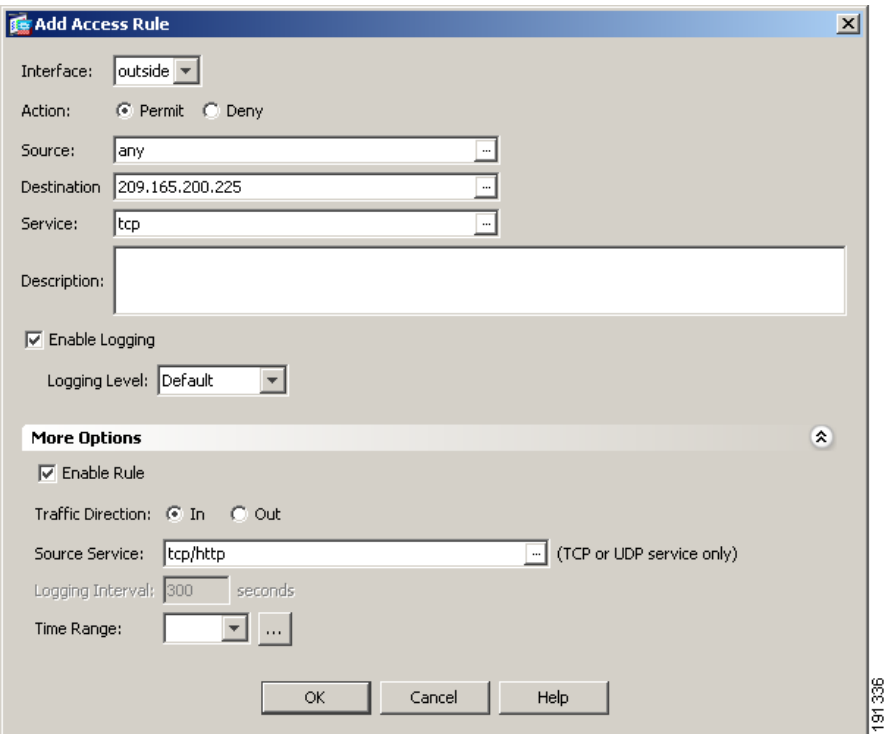
- **a.** Interface プルダウン リストで、outside を選択します。
- **b.** Permit Action オプション ボタンをクリックします。
- **c.** Source フィールドに any を入力します。
- **d.** Destination フィールドで、Web サーバのパブリック IP アドレス（209.165.200.225）を入力します。
- **e.** Service フィールドに tcp を入力します。
- **f.** More Options をクリックします。

g. アクセス コントロール規則をただちにイネーブルにする場合は、Enable Rule チェックボックスをオンにします。

h. Traffic Direction の隣で In をクリックします。

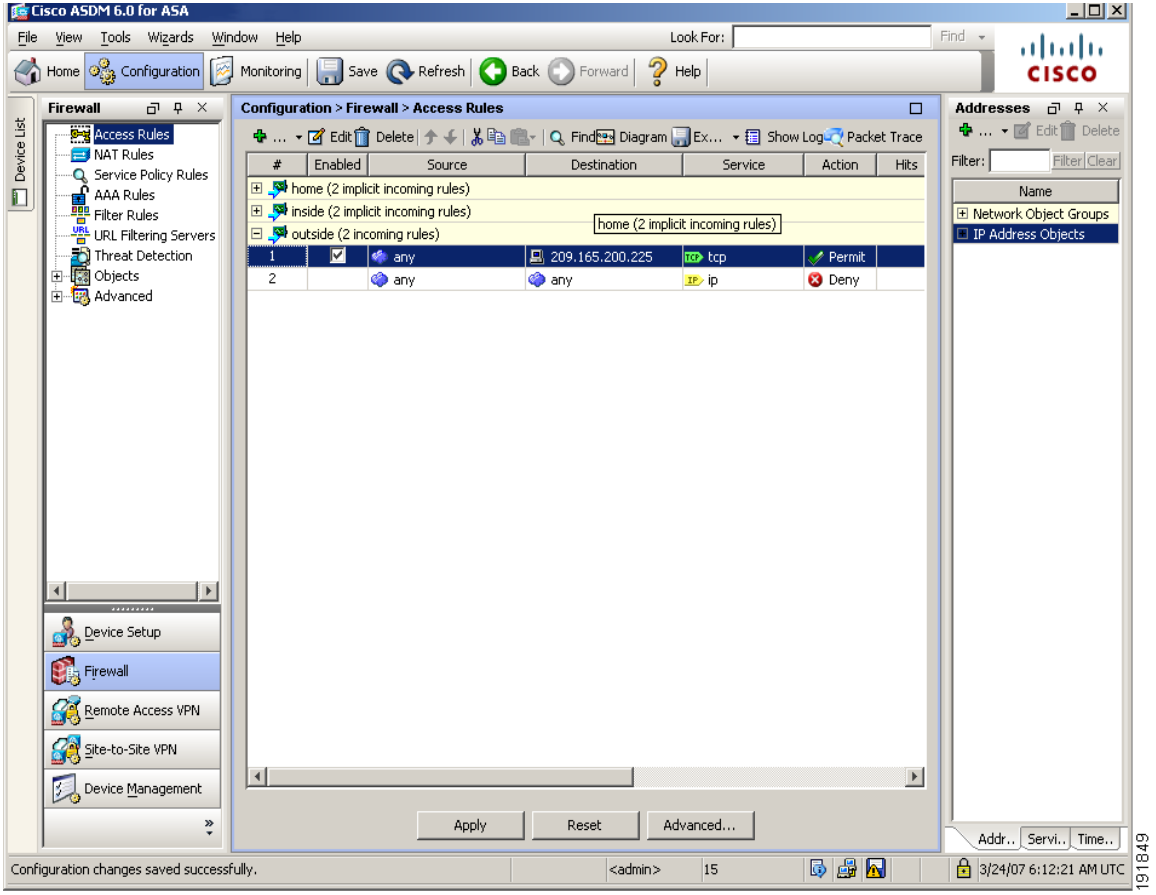
i. Source Service フィールドに tcp/http を入力します。

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。



j. **OK** をクリックし、Security Policy > Access Rules ペインに戻ります。

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。

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、パブリック ネットワーク上のクライアントが、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。

ステップ 3　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*

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 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
ブラウザベースの SSL VPN の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」

次の手順