CHAPTER 6

シナリオ：DMZ 設定

（注） Cisco ASA 5505 の DMZ 設定は、Security Plus ライセンスの場合にだけ可能です。

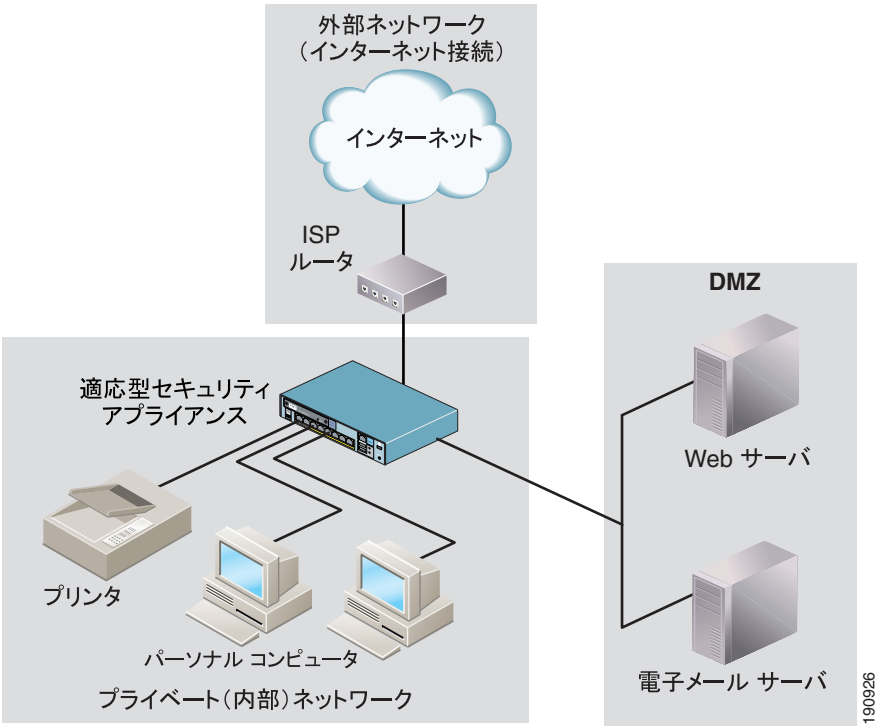
Demilitarized Zone（DMZ; 非武装地帯）は、プライベート（内部）ネットワークとパブリック（外部）ネットワークとの間の中立帯に位置する別個のネットワークです。

この章には、次の項があります。

DMZ 設定の基本的なネットワーク レイアウト

図 6-1 のネットワーク トポロジは、適応型セキュリティ アプライアンスの DMZ 実装で最も多く利用されているものです。この構成では、Web サーバは DMZ インターフェイス上にあり、内部ネットワークおよび外部ネットワークからの HTTP クライアントは Web サーバに安全にアクセスできます。

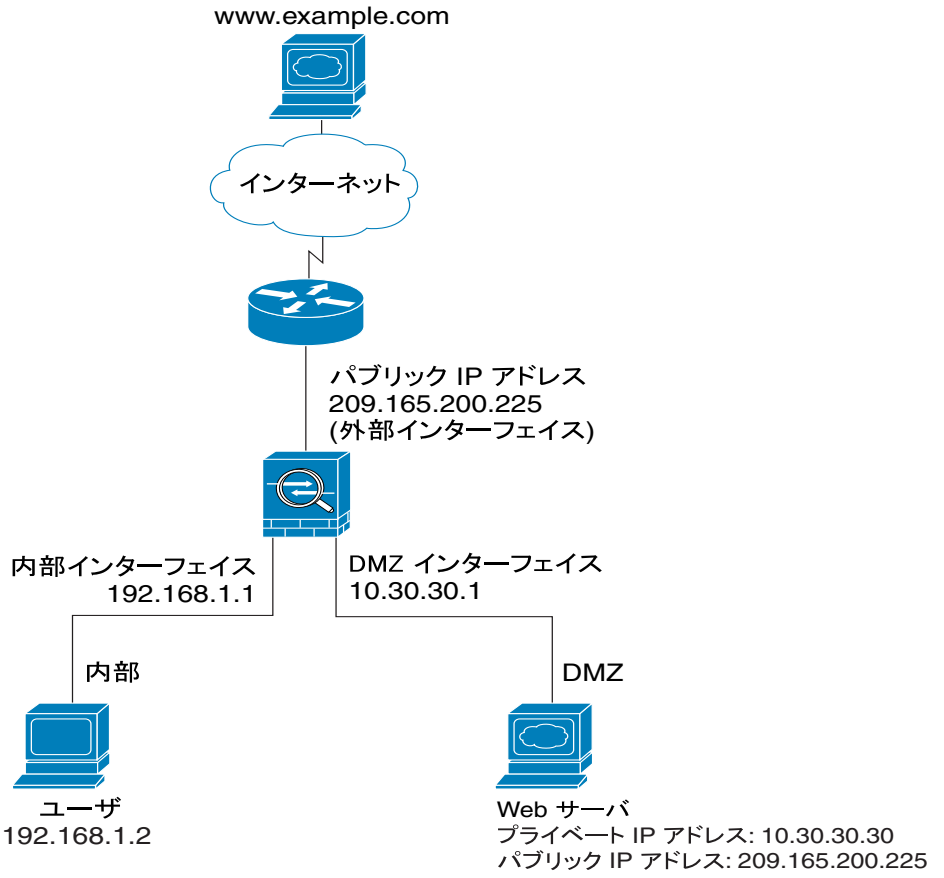
図 6-1　　DMZ を使用したプライベート ネットワーク



DMZ ネットワーク トポロジの例

この章では、図 6-2 に示すような適応型セキュリティ アプライアンスの DMZ 構成の設定方法について説明します。

図 6-2　DMZ 設定シナリオのネットワーク レイアウト



このシナリオ例には、次の特徴があります。

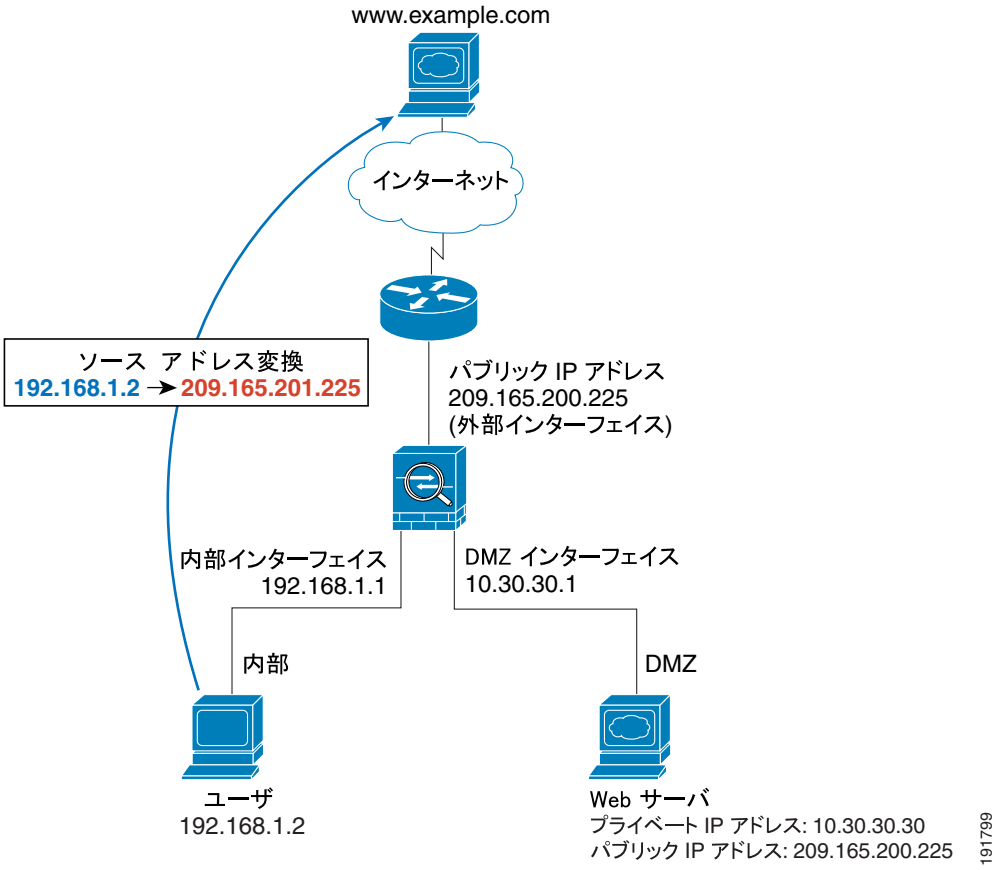
- Web サーバが適応型セキュリティ アプライアンスの DMZ インターフェイス上に存在します。
- プライベート ネットワーク上のクライアントは、DMZ 内の Web サーバにアクセスでき、インターネット上のデバイスとも通信できます。
- インターネット上のクライアントは、DMZ Web サーバへの HTTP アクセスが許可され、インターネットからのその他のトラフィックはすべて拒否されます。
- ネットワークには、だれでも使用できる IP アドレスが 1 つあります。この IP アドレスは適応型セキュリティ アプライアンスの外部インターフェイスです（209.165.200.225）。このパブリック アドレスは、適応型セキュリティ アプライアンスと DMZ Web サーバが共有します。

この項は、次の内容で構成されています。

内部ユーザによるインターネット上の Web サーバへのアクセス

図 6-3 に、内部ユーザがインターネット上の Web サーバから HTTP ページを要求したときに適応型セキュリティ アプライアンスを通って流れるトラフィックを示します。

図 6-3　内部ユーザによるインターネット Web サーバへのアクセス



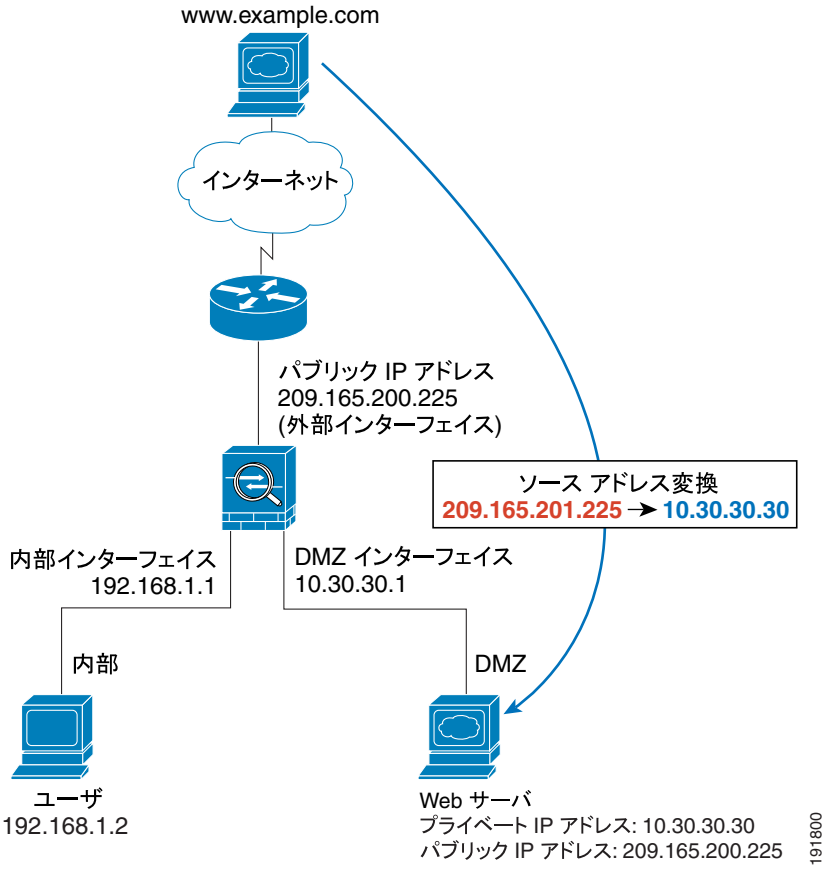
内部ユーザがインターネット上の Web サーバから HTTP ページを要求すると、データは次のように適応型セキュリティ アプライアンスを通って流れます。

1. 内部ネットワーク上のユーザが www.example.com から Web ページを要求します。
2. 適応型セキュリティ　アプライアンスがパケットを受信します。新しいセッションなので、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 アプライアンスがネットワーク アドレス変換（NAT）を実行し、ローカル ソース 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　アプライアンスが、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って流れます。
6. 適応型セキュリティ アプライアンスが、NAT を使用して、パブリック宛先アドレスをローカル ユーザ アドレスである 192.168.1.2 に変換します。
7. 適応型セキュリティ アプライアンスがパケットを内部ユーザに転送します。

インターネット ユーザによる DMZ Web サーバへのアクセス

図 6-4 に、インターネット上のユーザが DMZ Web サーバから Web ページを要求したときに適応型セキュリティ アプライアンスを通って流れるトラフィックを示します。

図 6-4　外部ユーザによる DMZ Web サーバへのアクセス



インターネット上のユーザが DMZ Web サーバから 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って流れます。

1. 外部ネットワーク上のユーザが、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（209.165.200.225、外部インターフェイスの IP アドレス）を使用して DMZ Web サーバから Web ページを要求します。
2. 適応型セキュリティ　アプライアンスがパケットを受信します。新しいセッションなので、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 アプライアンスが、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 ソース 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 アプライアンスがパケットを外部ユーザに転送します。

内部ユーザによる DMZ Web サーバへのアクセス

図 6-5 に、DMZ Web サーバにアクセスする内部ユーザを示します。

図 6-5　内部ユーザによる DMZ 上の Web サーバへのアクセス

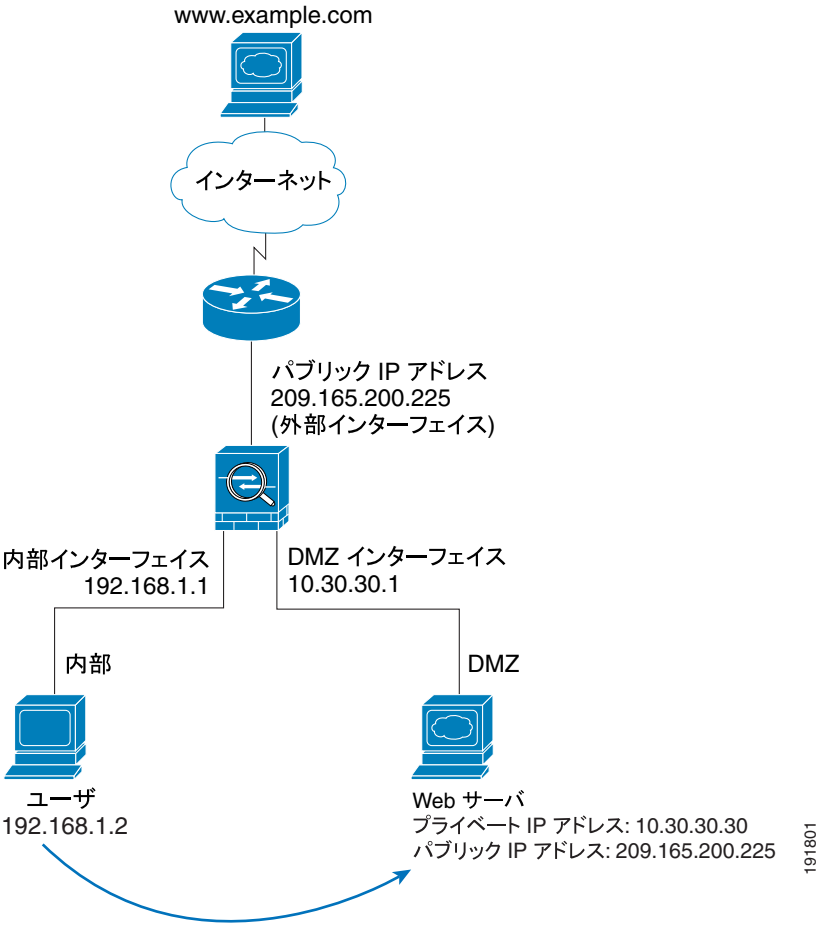


図 6-5 では、適応型セキュリティ アプライアンスは内部クライアントから DMZ Web サーバ宛の HTTP トラフィックを許可します。内部ネットワークには DNS サーバがないので、DMZ Web サーバへの内部クライアントの要求は、次のように処理されます。

1. ルックアップ要求が 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. 内部クライアントが、DMZ Web サーバのパブリック IP アドレスから Web ページを要求します。適応型セキュリティ アプライアンスが内部インターフェイス上で要求を受信します。
3. 適応型セキュリティ アプライアンスが、DMZ Web サーバのパブリック IP アドレスを実際のアドレスに変換し（209.165.200.225 -> 10.30.30.30）、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、そのデータを内部インターフェイスからユーザに転送します。

この設定を作成する手順については、この章の後半部分で説明します。

DMZ 構成用のセキュリティ アプライアンスの設定

この項では、ASDM を使用して、図 6-2 に示されている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、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 アプライアンスにはすでに内部インターフェイス、外部インターフェイス、および DMZ インターフェイスとして設定されているインターフェイスがあることを前提とします。ASDM で Startup Wizard を使用して、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設定します。DMZ インターフェイスのセキュリティ レベルを 0 ～ 100 の間に設定していることを確認します（通常は 50）。

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。

この項は、次の内容で構成されています。

この章の後半部分では、この設定を実装する方法について説明します。

設定要件

適応型セキュリティ アプライアンスのこの DMZ 構成には、次の設定ルールが必要です。

要件	作成するルール
内部クライアントがインターネット上の Web サーバから情報を要求できる	適応型セキュリティ アプライアンスは、内部クライアントによるインターネット上のデバイスへのアクセスを許可するように、デフォルトで設定されています。追加の設定は必要ありません。
内部クライアントが DMZ Web サーバから情報を要求できる	• DMZ Web サーバの実際の IP アドレスをパブリック IP アドレスに変換する（10.10.10.30 から 209.165.200.225 へ）、DMZ インターフェイスと内部インターフェイス間の NAT ルール。 • 内部クライアント ネットワークの実際のアドレスを変換する、内部インターフェイスと DMZ インターフェイス間の NAT ルール。このシナリオでは、内部クライアントが DMZ Web サーバと通信するとき、内部ネットワークの実際の IP アドレスは同じものに変換されます（10.10.10.0 から 10.10.10.0 へ）。
外部クライアントが DMZ Web サーバから情報を要求できる	• DMZ Web サーバのパブリック IP アドレスをプライベート IP アドレスに変換する（209.165.200.225 から 10.10.10.30 へ）、外部インターフェイスと DMZ インターフェイス間のアドレス変換ルール。 • 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 ルール。

収集する情報

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利用できるようにする、DMZ 内部のサーバ（このシナリオでは Web サーバ）の内部 IP アドレス
- DMZ 内部のサーバに使用するパブリック 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パブリック IP アドレスを使用して DMZ 内部のサーバにアクセスします）
- 発信トラフィックで内部 IP アドレスの代わりに使用されるクライアント 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表示され、内部 IP アドレスは公開されません）

ASDM の起動

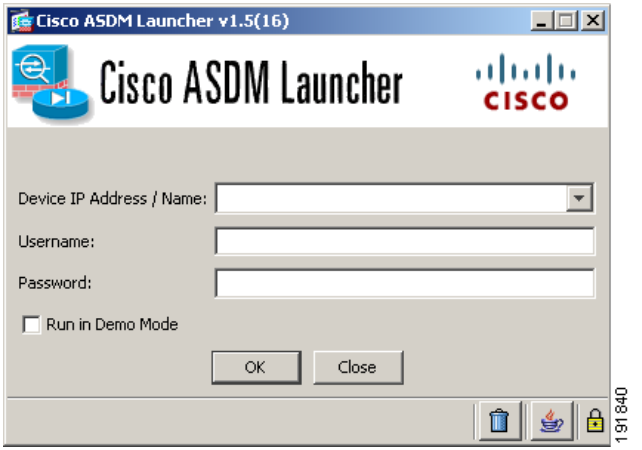
この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアがインストールされていない場合は、P.5-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して ASDM に直接アクセスする場合は、P.5-10 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、次の手順に従います。

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 と Password のフィールドは空白のままにしておきます。

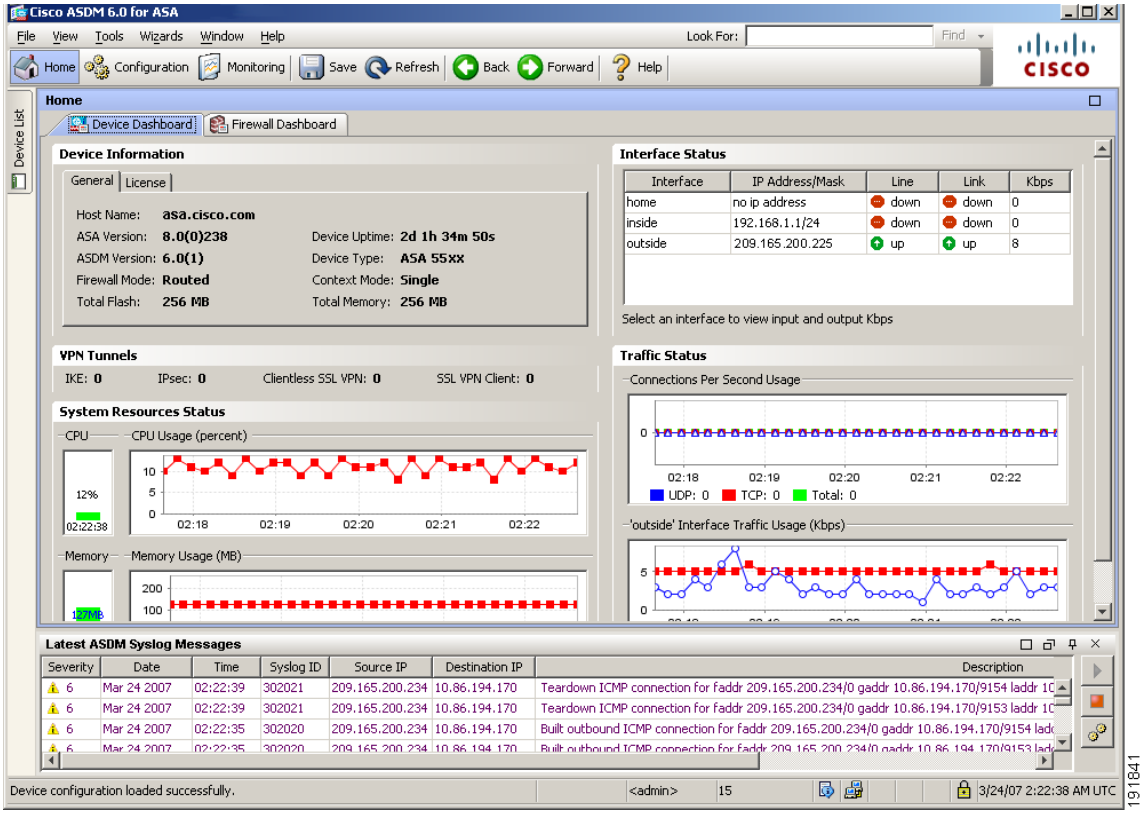
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書の受け入れ要求を含むセキュリティ警告が表示された場合は、**Yes** をクリックします。

ASA が、アップデートされたソフトウェアがあるかどうか確認し、ある場合は自動的にダウンロードします。

メイン ASDM ウィンドウが表示されます。



内部クライアントとインターネット上のデバイスとの通信を可能にする

内部クライアントによるインターネット上のデバイスからのコンテンツの要求を許可するには、適応型セキュリティ アプライアンスが内部クライアントの実際の 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表示されます。

ASA 5505 のデフォルト設定には、必要なアドレス変換ルールが含まれています。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 アクセスを許可するために何らかの設定を行う必要はありません。

内部クライアントと DMZ Web サーバとの通信を可能にする

この手順では、内部クライアントが DMZ 内の Web サーバと安全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。この手順を実行するには、次の 2 つの変換ルールを設定する必要があります。

- DMZ Web サーバの実際の IP アドレスをパブリック IP アドレスに変換する（10.30.30.30 から 209.165.200.225 へ）、DMZ インターフェイスと内部インターフェイス間の NAT ルール。
- DMZ Web サーバのパブリック IP アドレスを実際の IP アドレスに変換する（209.165.200.225 から 10.30.30.30 へ）、内部インターフェイスと DMZ インターフェイス間の NAT ルール。

  このルールが必要なのは、内部クライアントが DNS ルックアップ要求を送信したときに、DNS サーバが DMZ Web サーバのパブリック IP アドレスを返すためです。

（注） 内部ネットワーク上には DNS サーバがないため、DNS 要求は適応型セキュリティ アプライアンスから出て、インターネット上の DNS サーバによって解決されなければなりません。

この項は、次の内容で構成されています。

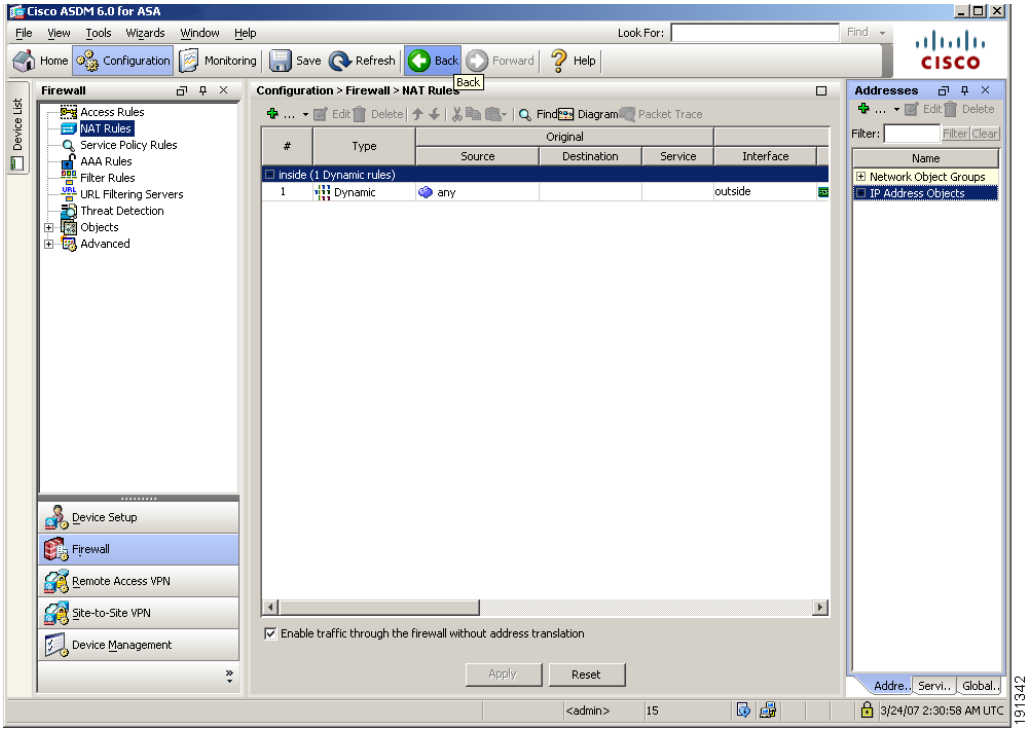
内部インターフェイスと DMZ インターフェイス間の内部クライアント IP アドレスの変換

内部インターフェイスと DMZ インターフェイス間で内部クライアント IP アドレスを変換するように NAT を設定するには、次の手順に従います。

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

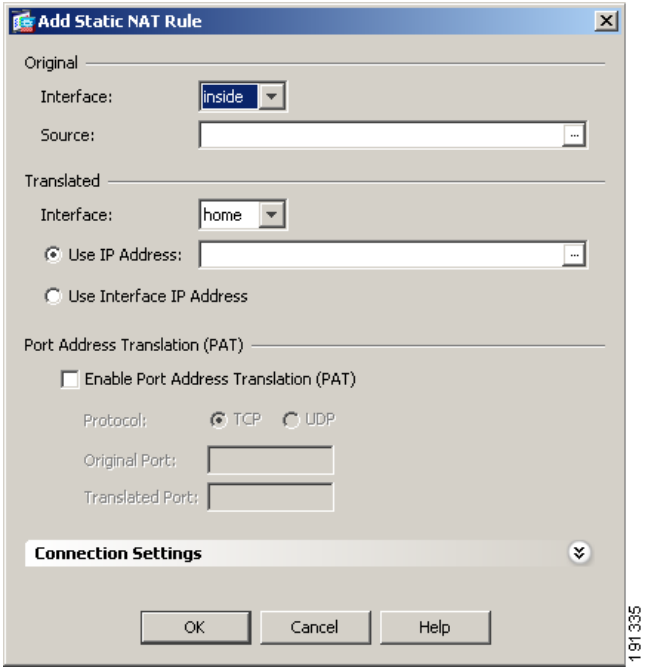
ステップ 2　ASDM ウィンドウの左側にある Device List 領域で、Firewall をクリックします。

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（+）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、内部クライアント用のアドレス変換は、10.10.10.0 サブネット全体に対して実行されます。

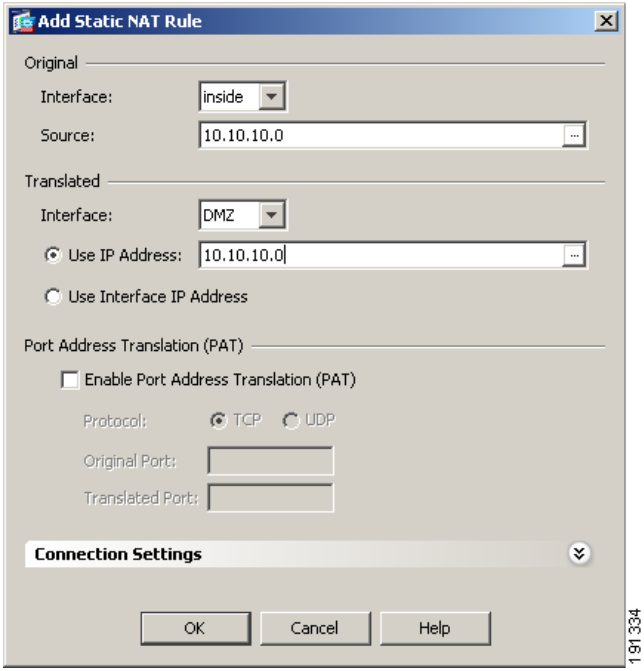
a.　Interface ドロップダウン リストから、Inside インターフェイスを選択します。

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、次の内容を実行します。

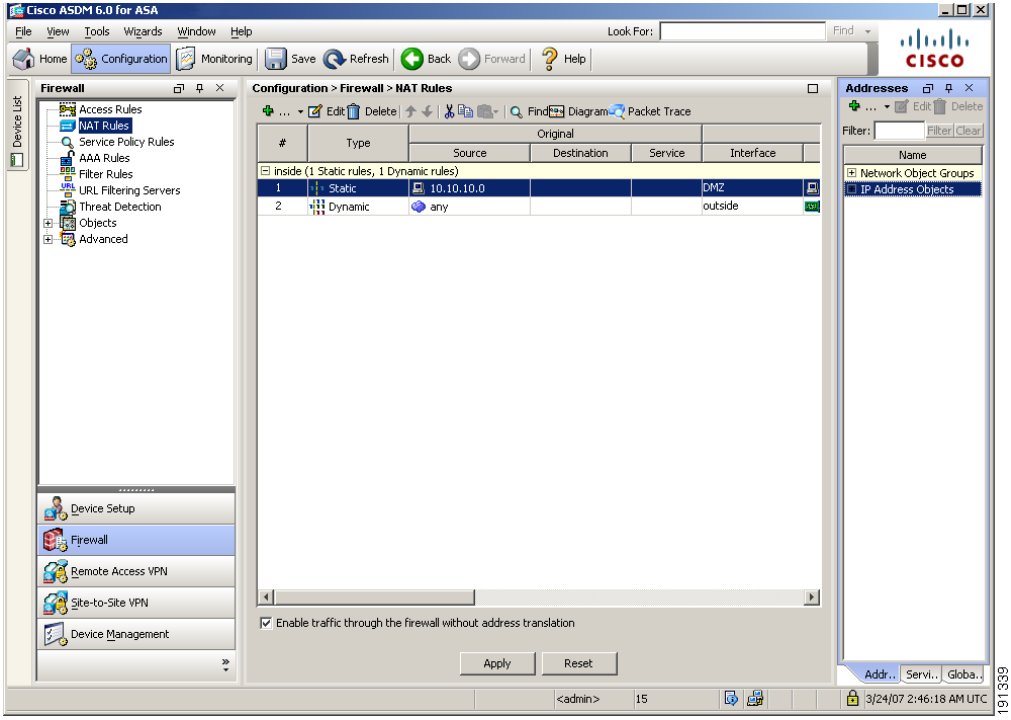
a. Interface ドロップダウン リストから、DMZ インターフェイスを選択します。

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。

変換ルールが意図したとおりに表示されていることを設定ペインで確認します。ルール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終了します。

Web サーバのパブリック アドレスから実際のアドレスへの変換

Web サーバのパブリック IP アドレスを実際のアドレスに変換する NAT ルールを設定するには、次の手順に従います。

ステップ 1　Configuration > Firewall > NAT Rules 画面で、緑色のプラス (+) 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、次の内容を実行します。

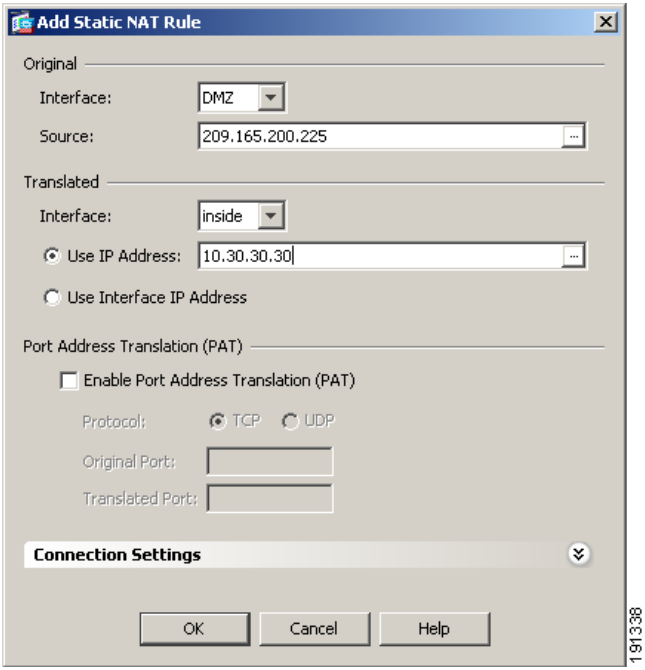
a. Interfaces ドロップダウン リストから、DMZ を選択します。

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

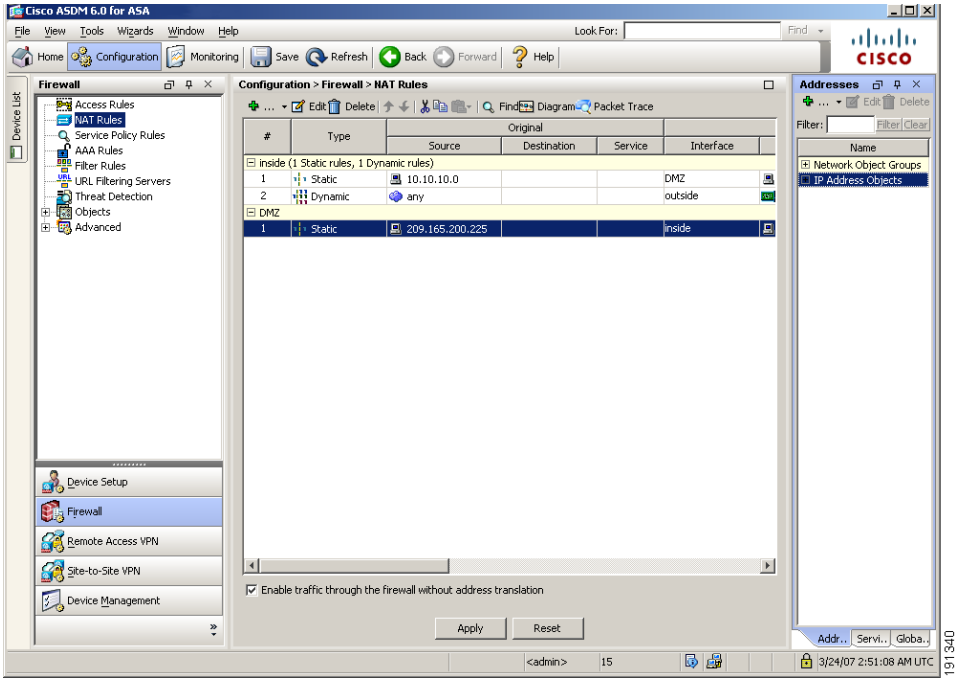
ステップ 3　Translated 領域で、次の内容を実行します。

a. Interface ドロップダウン リストから、Inside を選択します。

b. IP Address ドロップダウン リストから、DMZ Web サーバの実際の IP アドレスを選択するか、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 4　**OK** をクリックして、Configuration > NAT ペインに戻ります。設定は次のように表示されます。



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終了します。

DMZ Web サーバへのパブリック アクセス（ポート転送）用のスタティック PAT 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、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 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とパブリック IP アドレス（209.165.200.225）を共有します。

実際の 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するには、次の手順に従います。

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。

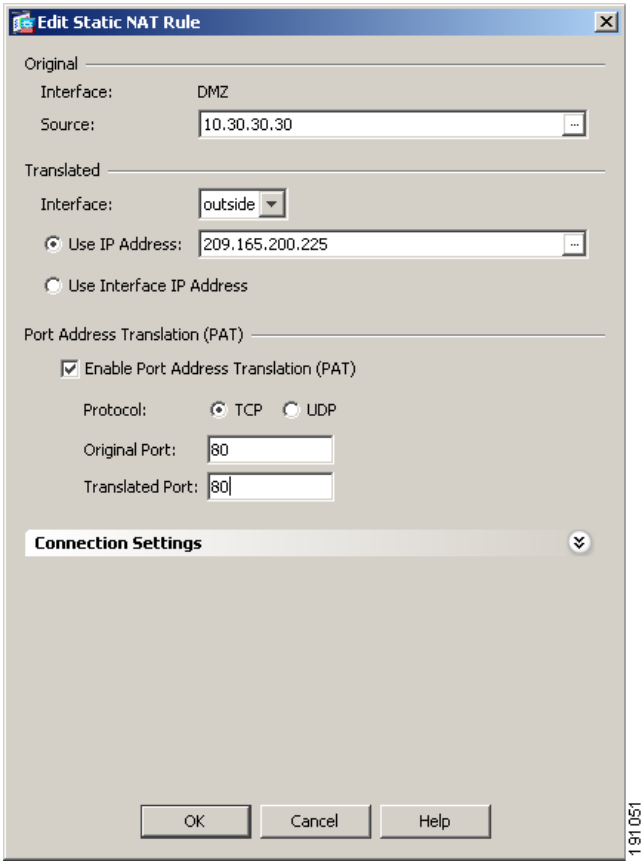
Add Static NAT Rule ダイアログボックスが表示されます。

ステップ 2　Original 領域で、Web サーバの実際の IP アドレスを指定します。

a. Interface ドロップダウン リストから、DMZ インターフェイスを選択します。
b. DMZ Web サーバの実際の 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 10.30.30.30 です。

ステップ 3　Translated 領域で、Web サーバで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 リストから、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。これは、指定したインターフェイスの IP アドレス、つまり、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　Port Address Translation を設定します。

パブリック IP アドレスは 1 つだけなので、Port Address Translation 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。Port Address Translation を設定するには、次の手順に従います。

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。

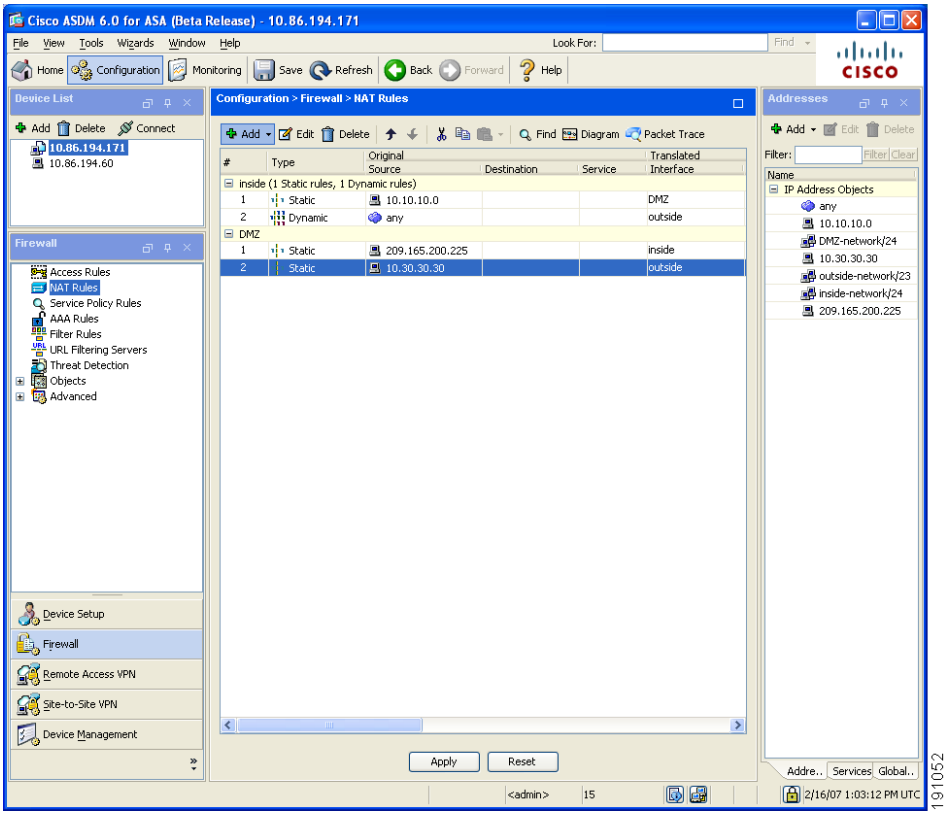
c. Original Port フィールドに 80 と入力します。

d. Translated Port フィールドに 80 と入力します。

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

このルールは、実際の 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（209.165.200.225）にスタティックにマッピングします。

ステップ 5　ルールが、意図したと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終了します。

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 ネットワークから着信するトラフィックをすべて拒否します。インターネットから DMZ Web サーバにアクセスするトラフィックを許可するには、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 ル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 ルールは、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に対して、トラフィックが着信されるかどうか、トラフィックの発信元および宛先、および許可するトラフィック プロトコルとサービスのタイプを指定します。

この項では、トラフィックの宛先が DMZ ネットワークの Web サーバである場合に、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 ルールを作成します。パブリック ネットワークから着信する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 ルールを設定するには、次の手順に従います。

ステップ 1　メイン ASDM ウィンドウで、次の内容を実行します。

- **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 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、次の内容を実行します。

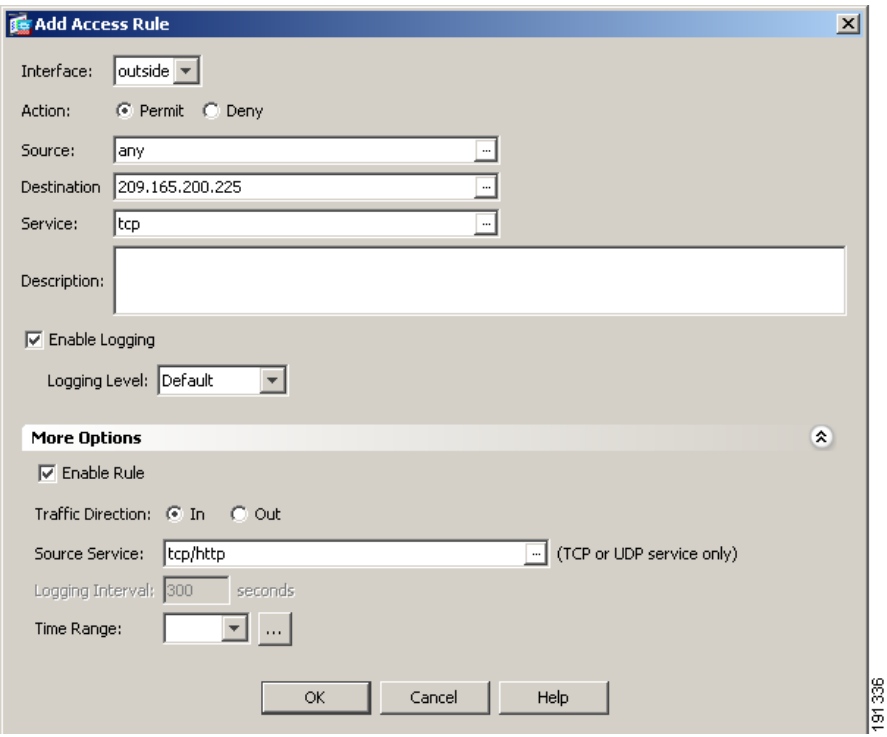
- **a.** Interface プルダウン リストから、Outside を選択します。
- **b.** Permit Action オプション ボタンをクリックします。
- **c.** Source フィールドに Any と入力します。
- **d.** Destination フィールドに Web サーバのパブリック IP アドレス（209.165.200.225）を入力します。
- **e.** Service フィールドに TCP と入力します。
- **f.** More Options をクリックします。

g. このアクセス コントロール ルールをすぐに有効にする場合は、Enable Rule チェックボックスをオンにします。

h. Traffic Direction の隣の In をクリックします。

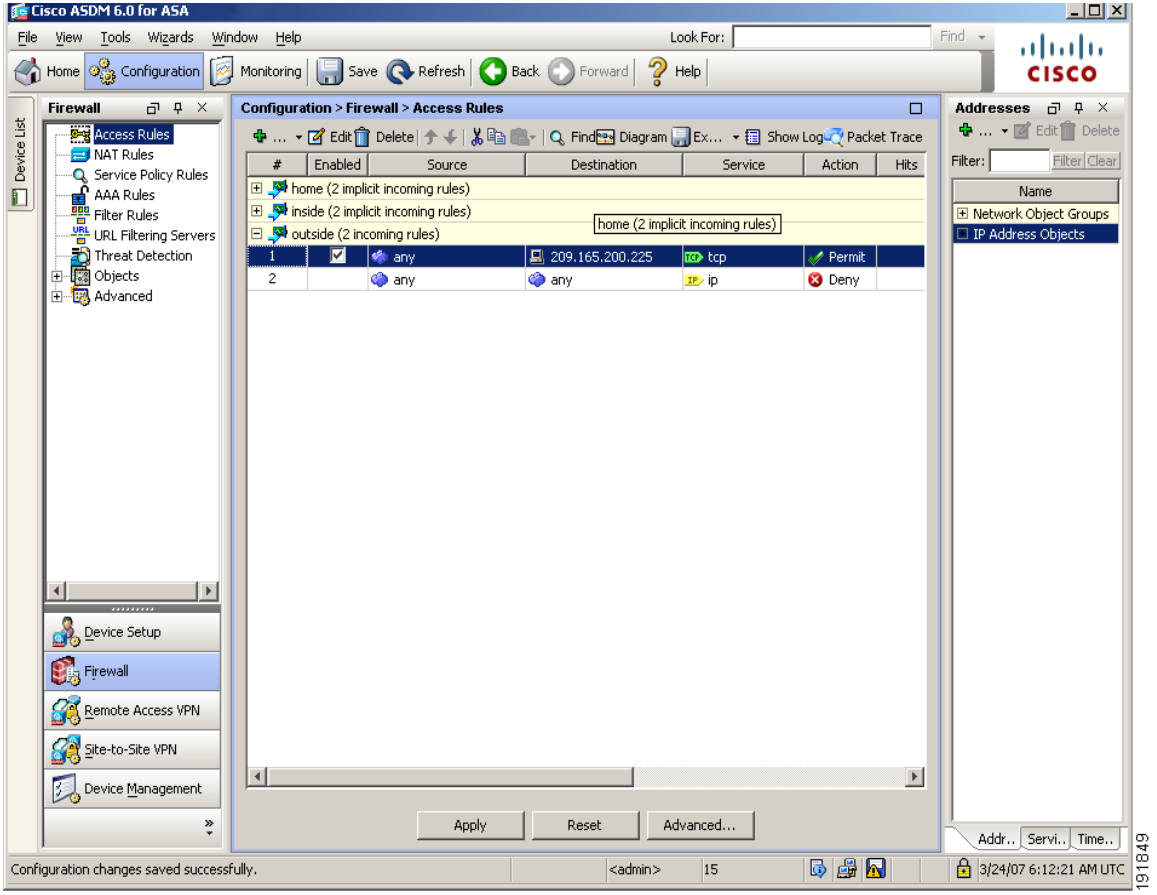
i. Source Service フィールドに tcp/http と入力します。

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** をクリックして、**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、適応型セキュリティ アプライアンスを現在実行している設定に設定変更を保存します。

これで、プライベート ネットワークに存在するクライアントは、DMZ Web サーバからのコンテンツに対する HTTP 要求を解決できるだけでなく、プライベート ネットワークの安全性を保持できるようになりました。

ステップ 3　次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、File メニューから **Save** をクリックします。

または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

次の作業

DMZ 内の Web サーバを保護するためだけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が完了しました。次の追加の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常的な運用について	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
リモートアクセス VPN の設定	第 7 章「シナリオ：IPsec リモートアクセス VPN 設定」
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 8 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
ブラウザベースの SSL VPN の設定	第 9 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 10 章「シナリオ:サイトツーサイト VPN 設定」

次の作業