



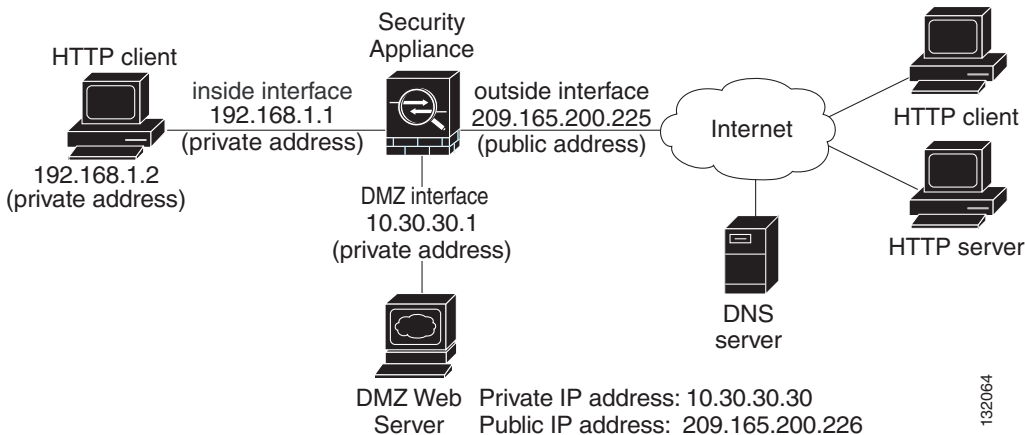
## Scenario: DMZ Configuration

---

A demilitarized zone (DMZ) is a separate network located in the neutral zone between a private (inside) network and a public (outside) network. This example network topology is similar to most DMZ implementations of the adaptive security appliance. The web server is on the DMZ interface, and HTTP clients from both the inside and outside networks can access the web server.

In [Figure 6-1](#), an HTTP client (192.168.1.2) on the inside network initiates HTTP communications with the DMZ web server (10.30.30.30). HTTP access to the DMZ web server is provided for all clients on the Internet; all other communications are denied. The network is configured to use an IP pool of addresses between 10.30.30.50 and 10.30.30.60. (The IP pool is the range of IP addresses available to the DMZ interface.)

**Figure 6-1** Network Layout for DMZ Configuration Scenario



Because the DMZ web server is located on a private DMZ network, it is necessary to translate its private IP address to a public (routable) IP address. This public address allows external clients to access the DMZ web server in the same way that they access any server on the Internet.

The DMZ configuration scenario shown in [Figure 6-1](#) provides two routable IP addresses that are publicly available: one for the outside interface (209.165.200.225) of the adaptive security appliance, and one for the public IP address of the DMZ web server (209.165.200.226). The following procedures describe how to use ASDM to configure the adaptive security appliance for secure communications between HTTP clients and the web server.

In this DMZ scenario, the adaptive security appliance already has an outside interface configured, called **dmz**. Set up the adaptive security appliance interface for your DMZ by using the Startup Wizard. Ensure that the security level is set between 0 and 100. (A common choice is 50.)

## Implementing the DMZ Scenario

The following sections provide instructions for configuring the adaptive security appliance in a DMZ deployment, using example parameters from the scenario illustrated in [Figure 6-1](#).

## Information to Have Available

Before you begin this configuration procedure, gather the following information:

- Internal IP addresses of the servers inside the DMZ that you want to make available to clients on the public network (in this scenario, a web server).
- Public IP addresses to be used for servers inside the DMZ. (Clients on the public network will use the external IP address to access the server inside the DMZ.)
- Client IP address to substitute for internal IP addresses in outgoing traffic. (Outgoing client traffic will appear to come from this address so that the internal IP address is not exposed.)

## Configuring the Security Appliance for a DMZ Deployment

This procedure describes the configuration steps you must take to configure the adaptive security appliance to protect a web server in a DMZ. The procedure uses the network topology shown in [Figure 6-1](#) as the example deployment, and includes the following steps:

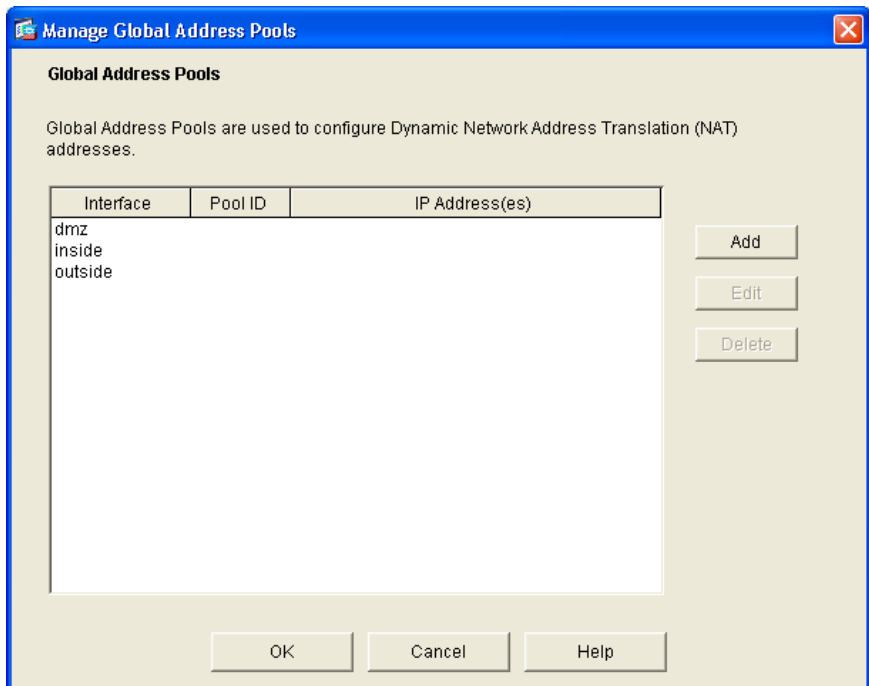
1. [Configure IP Pools for Network Translations.](#)
2. [Configure Address Translations on Private Networks.](#)
3. [Configure External Identity for the DMZ Web Server.](#)
4. [Provide HTTP Access to the DMZ Web Server.](#)

### Configure IP Pools for Network Translations

For an inside HTTP client (192.168.1.0) to access the web server on the DMZ network (10.30.30.30), it is necessary to define a pool of IP addresses for the DMZ interface (10.30.30.50–10.30.30.60). Similarly, an IP pool for the outside interface (209.165.200.225) is required for the inside HTTP client to communicate with any device on the public network. Use ASDM to manage IP pools efficiently and to facilitate secure communications between protected network clients and devices on the Internet.

To configure IP pools for network translation, perform the following steps:

- Step 1** At the top of the ASDM window, click the **Configuration** tab, then click the **NAT** feature on the left side of the ASDM window.
- Step 2** At the bottom of the ASDM window, click **Manage Pools**. The Manage Global Address Pools dialog box appears, allowing you to add or edit global address pools.



**Note** For most configurations, global pools are added to the less secure, or public, interfaces.

- Step 3** In the Manage Global Address Pools dialog box:
- Click the **dmz** interface (configured using the Startup Wizard before beginning this procedure).

- b. Click **Add**. The Add Global Pool Item dialog box appears.

The screenshot shows the 'Add Global Pool Item' dialog box with the following configuration:

- Interface: dmz
- Pool ID: 200
- Selected option: Range
- IP Address range: 10.30.30.50 to 10.30.30.60
- Network Mask (optional): 255.255.255.224

Buttons: OK, Cancel, Help

92596

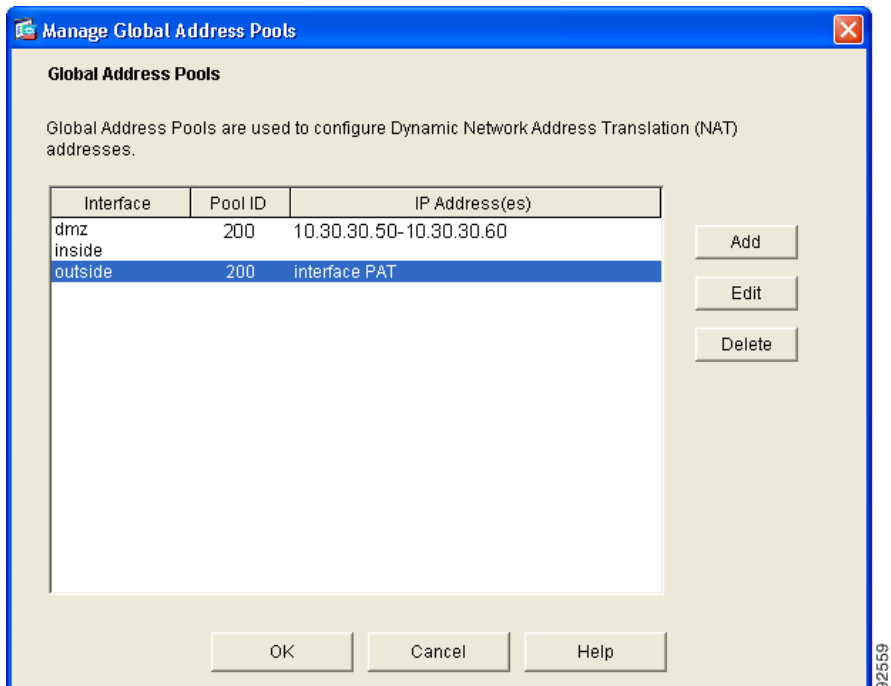
- Step 4** In the Add Global Pool Item dialog box:
- a. From the Interface drop-down list, click **dmz**.
  - b. Click **Range** to enter the IP address range.
  - c. Enter the range of IP addresses for the DMZ interface. In this scenario, the range is 10.30.30.50 to 10.30.30.60.
  - d. Enter a unique Pool ID. In this scenario, the Pool ID is 200.
  - e. Click **OK** to return to the Manage Global Address Pools dialog box.

**Note**

You can also click **Port Address Translation (PAT)** or **Port Address Translation (PAT) using the IP address of the interface** if there are limited IP addresses available for the DMZ interface.

## Implementing the DMZ Scenario

- Step 5** In the Manage Global Address Pools dialog box:
- Click the **outside** interface.
  - Click **Add**.
- Step 6** When the Add Global Pool Item dialog box appears:
- From the Interface drop-down list, click **outside**.
  - Click **Port Address Translation (PAT) using the IP address of the interface**.
  - Assign the same Pool ID for this pool as you did in Step 5d. (For this scenario, the Pool ID is 200.)
  - Click **OK**. The displayed configuration should be similar to the following:



- Step 7** Confirm that the configuration values are correct, then:
- Click **OK**.

- b. Click **Apply** in the main ASDM window.

**Note**

---

Because there are only two public IP addresses available, with one reserved for the DMZ server, all traffic initiated by the inside HTTP client exits the adaptive security appliance using the outside interface IP address. This configuration allows traffic from the inside client to be routed to and from the Internet.

---

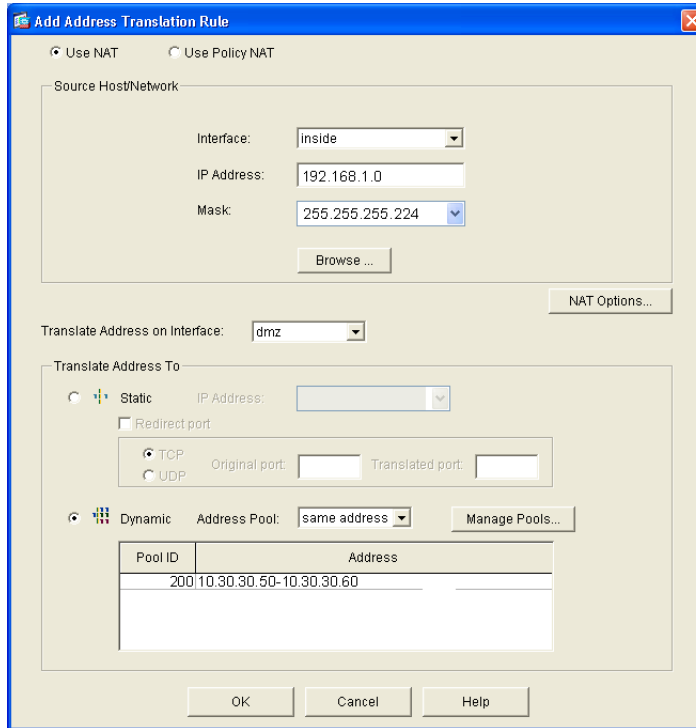
## Configure Address Translations on Private Networks

Network Address Translation (NAT) replaces the source IP addresses of network traffic exchanged between two interfaces on the adaptive security appliance. This translation permits routing through the public networks while preventing internal IP addresses from being exposed on the public networks.

Port Address Translation (PAT) is an extension of the NAT function that allows several hosts on a private network to map into a single IP address on the public network. PAT is essential for small and medium businesses that have a limited number of public IP addresses available to them.

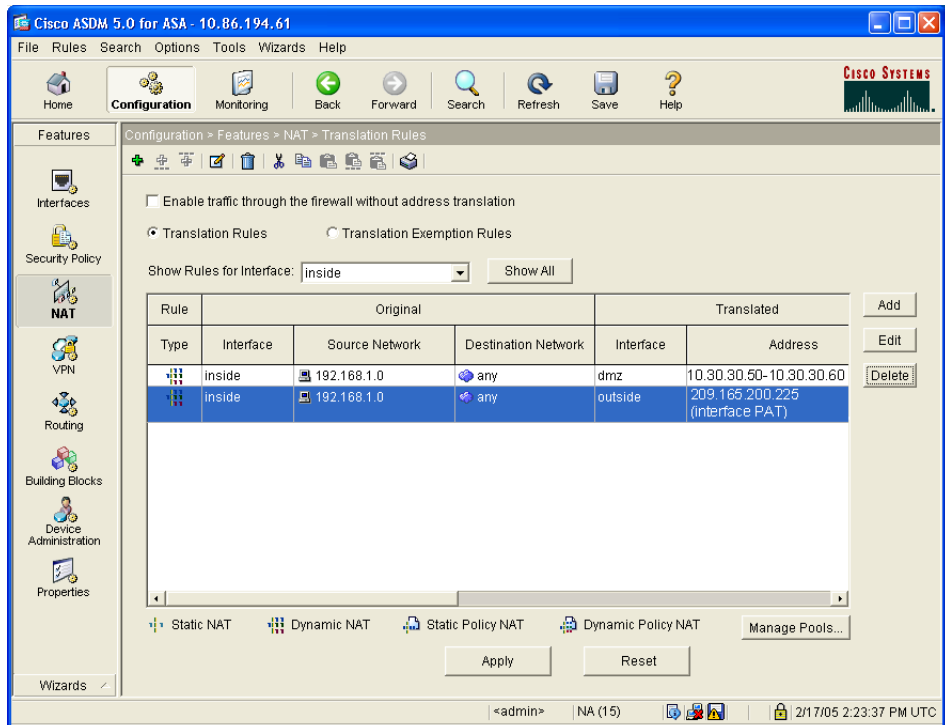
To configure NAT between the inside interface and the DMZ interface for the inside HTTP client, perform the following steps starting from the main ASDM window:

- 
- Step 1** At the top of the ASDM window, click the **Configuration** tab.
  - Step 2** On the left side of the ASDM window, click the **NAT** tab.
  - Step 3** Click **Translation Rules**, and then click **Add** on the right side of the ASDM window.
  - Step 4** In the Add Address Translation Rule dialog box, click the **Use NAT** radio button, and then click the **inside** interface.



- Step 5** Enter the IP address of the inside client. In this scenario, the IP address is **192.168.1.0**.
- Step 6** From the Mask drop-down list, choose **255.255.255.224**.
- Step 7** From the Translate Address on Interface drop-down list, choose the DMZ interface.
- Step 8** In the Translate Address To area, click **Dynamic**.
- Step 9** From the Address Pools drop-down list, click **200**.
- Step 10** Click **OK**.
- Step 11** A dialog box appears asking if you want to proceed. Click **Proceed**.
- Step 12** On the NAT Translation Rules window, check the displayed configuration for accuracy.
- Step 13** Click **Apply** to complete the adaptive security appliance configuration changes.

The displayed configuration should be similar to the following:



132195

## Configure External Identity for the DMZ Web Server

The DMZ web server needs to be easily accessible by all hosts on the Internet. This configuration requires translating the IP address of the web server so that it appears to be located on the Internet, enabling outside HTTP clients to access it unaware of the adaptive security appliance. Perform the following steps to map the web server IP address (10.30.30.30) statically to a public IP address (209.165.200.225):

- Step 1** On the top of the ASDM window, click the **Configuration** tab.

## Implementing the DMZ Scenario

- Step 2** On the left side of the ASDM window, click the **NAT** tab.
- Step 3** Click **Translation Rules**, then click **Add** on the right side of the window.
- Step 4** In the Add Translation Rule dialog box, select the **Use NAT** radio button and then, from the drop-down list of interfaces, select the outside dmz interface.
- Step 5** Enter the private IP address (10.30.30.30) for the DMZ web server.
- Step 6** From the Mask drop-down list, click **255.255.255.224**.
- Step 7** In the Translate Address To area, click **Static**.
- Step 8** Enter the external IP address (209.165.200.226) for the DMZ web server. Then click **OK**.
- Step 9** Verify the values that you entered, then click **Apply**.

The displayed configuration should be similar to the following:

The screenshot shows the Cisco ASDM 5.0 interface for ASA configuration. The left sidebar has the **NAT** tab selected. The main window displays the **Translation Rules** configuration page. The **Translation Rules** radio button is selected. The **Show Rules for Interface:** dropdown is set to **All Interfaces**. The table below shows the configured NAT rules:

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	outside	10.30.30.30	any	inside	209.165.200.226
	inside	192.168.1.0	any	dmz	10.30.30.50-10.30.30.60
	inside	192.168.1.0	any	outside	209.165.200.225 (Interface PAT)

At the bottom of the window, the status bar shows: Device configuration loaded successfully. <admin> | NA (15) | 2/17/05 8:02:37 PM UTC

132196

## Provide HTTP Access to the DMZ Web Server

By default, the adaptive security appliance denies all traffic coming in from the public network. You must create access control rules on the adaptive security appliance to allow specific traffic types from the public network through the adaptive security appliance to resources in the DMZ.

To configure an access control rule that allows HTTP traffic through the adaptive security appliance so that any client on the Internet can access a web server inside the DMZ, perform the following steps:

---

**Step 1** In the ASDM window:

- a. Click **Configuration**.
- b. On the left side of the ASDM window, click **Security Policy**.
- c. In the table, click **Add**.

**Step 2** In the Add Access Rule dialog box:

- a. In the Action area, click **permit** from the drop-down list to allow traffic through the adaptive security appliance.
- b. In the Source Host/Network area, click **IP Address**.
- c. From the Interface drop-down list, click **outside**.
- d. Enter the IP address of the Source Host/Network information. (Use 0.0.0.0 to allow traffic originating from any host or network.)
- e. In the Destination Host/Network area, click **IP Address**.
- f. From the Interface drop-down list, click the **dmz** interface.
- g. In the IP address field, enter the IP address of the destination host or network, such as a web server. (In this scenario, the public IP address of the web server is 209.165.200.226.)
- h. From the Mask drop-down list, click **255.255.255.224**.



**Note**

---

Alternatively, you can click the Hosts/Networks in both cases by clicking the respective **Browse** buttons.

---

**Step 3** Specify the type of traffic that you want to permit.



**Note** HTTP traffic is always directed from any TCP source port number toward a fixed destination TCP port number 80.

- a. In the Protocol and Service area, click **TCP**.
- b. In the Source Port area, click “=” (equal to) from the **Service** drop-down list.
- c. Click the button labeled with ellipses (...), scroll through the options, and then click **Any**.
- d. In the Destination Port area, click “=” (equal to) from the **Service** drop-down list.

- e. Click the button labeled with ellipses (...), scroll through the options, and then click **HTTP**.
- f. Click **OK**.

**Note**

---

For additional features, such as logging system messages by ACL, click **More Options** at the top at the top of the window. You can provide a name for the access rule in the dialog box at the bottom.

---

- g. Verify that the information you entered is accurate, and then click **OK**.

**Note**

---

Although the destination address specified is the private address of the DMZ web server (10.30.30.30), HTTP traffic from any host on the Internet destined for 209.165.200.225 is permitted through the adaptive security appliance. The address translation (10.30.30.30 = 209.165.200.225) allows the traffic to be permitted.

---

- h. Click **Apply** in the main ASDM window.

The displayed configuration should be similar to the following:

The screenshot shows the Cisco ASDM 5.0 interface for configuration. The main window displays the 'Security Policy > Access Rules' configuration page. The 'Access Rules' tab is selected, and the 'Show Rules for Interface' is set to 'All Interfaces'. The table below shows the configured rules:

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	any	any		inside (outbound)	ip
-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	any	any		dmz (outbound)	ip
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	any	209.165.200.226	Incoming	outside	http/tcp

At the bottom of the window, there are buttons for 'Apply', 'Reset', and 'Advanced...'. The status bar shows the user is 'admin' on 'NA (15)' with a timestamp of '2/17/05 8:21:47 PM UTC'.

The HTTP clients on both the private and public networks can now access the DMZ web server securely.

## What to Do Next

If you are deploying the adaptive security appliance solely to protect a web server in a DMZ, you have completed the initial configuration. You may want to consider performing some of the following additional steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	<a href="#">Cisco Security Appliance Command Line Configuration Guide</a>
Learn about daily operations	<a href="#">Cisco Security Appliance Command Reference</a> <a href="#">Cisco Security Appliance Logging Configuration and System Log Messages</a>
Review hardware maintenance and troubleshooting information	<a href="#">Cisco ASA 5500 Series Hardware Installation Guide</a>

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This ...	See ...
Configure a remote-access VPN	<a href="#">Chapter 7, “Scenario: Remote-Access VPN Configuration”</a>
Configure a site-to-site VPN	<a href="#">Chapter 8, “Scenario: Site-to-Site VPN Configuration”</a>

