



Scenario: DMZ Configuration



Note

Cisco ASA 5505 DMZ configurations are possible only with the Security Plus license.

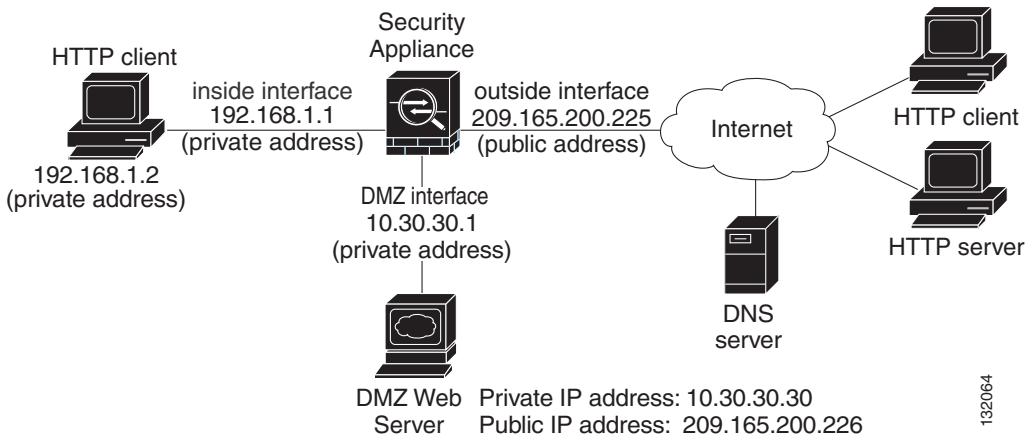
This chapter includes the following sections:

- [Example DMZ Network Topology, page 6-1](#)
- [Configuring the Security Appliance for a DMZ Deployment, page 6-5](#)
- [What to Do Next, page 6-16](#)

Example DMZ Network Topology

The example network topology shown in [Figure 6-1](#) is typical of many DMZ implementations of the adaptive security appliance.

Figure 6-1 Network Layout for DMZ Configuration Scenario

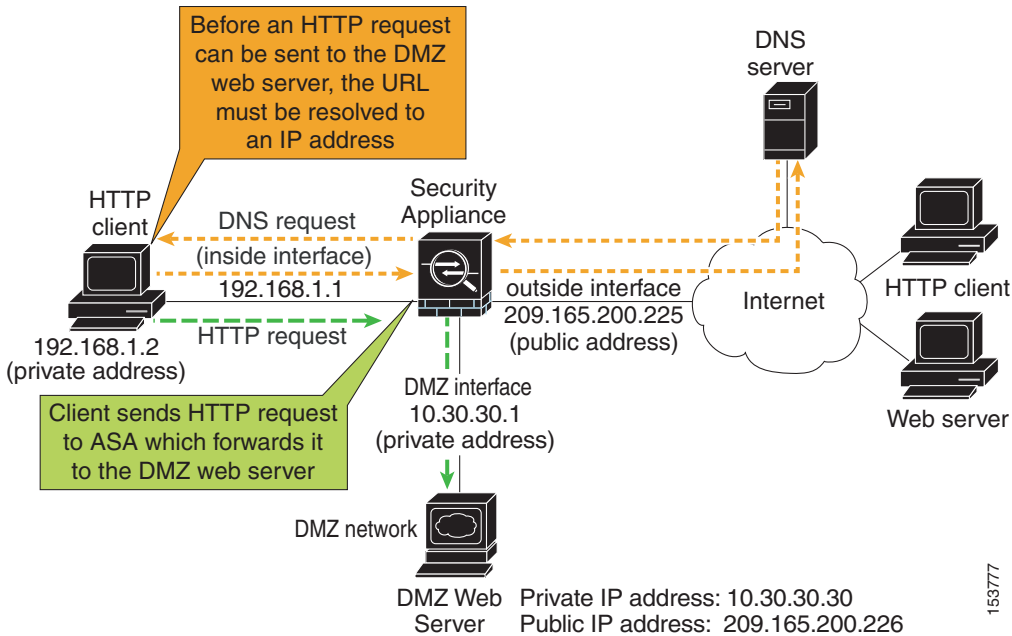


This example scenario has the following characteristics:

- The web server is on the DMZ interface of the adaptive security appliance.
- HTTP clients on the inside network can access the web server in the DMZ and can also communicate with devices on the Internet.
- Clients on the Internet are permitted HTTP access to the DMZ web server; all other traffic is denied.
- The network has one routable IP address that is publicly available: the outside interface of the adaptive security appliance (209.165.200.225).

Figure 6-2 shows the outgoing traffic flow of HTTP requests from the private network to both the DMZ web server and to the Internet.

Figure 6-2 Outgoing HTTP Traffic Flow from the Private Network



In Figure 6-2, the adaptive security appliance permits HTTP traffic originating from inside clients and destined for the DMZ web server. Because the internal network does not include a DNS server, internal client requests for the DMZ web server are handled as follows:

1. A lookup request is sent to the DNS server of the ISP. The public IP address of the DMZ web server is returned to the client.
2. The internal client sends the HTTP request to the adaptive security appliance.
3. The adaptive security appliance translates the public IP address of the DMZ web server to its real address and forwards the request to the web server.
4. The DMZ web server returns the HTTP content to the adaptive security appliance with a destination address of the real IP address of the internal client.

- The adaptive security appliance forwards the HTTP content to the internal client.

To permit internal clients to request HTTP content from the DMZ web server, the adaptive security appliance configuration must include the following rules:

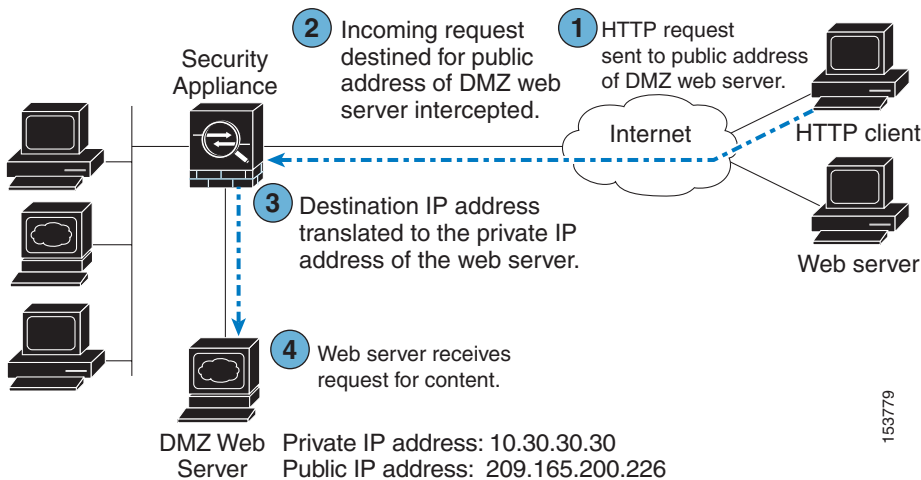
- A NAT rule between the DMZ and inside interfaces that translates the real IP address of the DMZ web server to the public IP address of the DMZ web server (10.30.30.30 to 209.165.200.225).
- A NAT rule between the inside and DMZ interfaces that translate the real addresses of the internal client network. In this scenario, the real IP address of the internal network is translated to itself when internal clients communicate with the web server in the DMZ (10.30.30.30 to 10.30.30.30).

To permit traffic coming from the Internet to access the DMZ web server, the adaptive security appliance configuration includes the following:

- An address translation rule translating the public IP address of the DMZ web server to the private IP address of the DMZ web server.
- An access control rule permitting incoming HTTP traffic that is destined for the DMZ web server.

Figure 6-3 shows HTTP requests originating from the Internet and destined for the public IP address of the DMZ web server.

Figure 6-3 Incoming HTTP Traffic Flow From the Internet



The procedures for creating this configuration are detailed in the remainder of this chapter.

Configuring the Security Appliance for a DMZ Deployment

This section describes how to use ASDM to configure the adaptive security appliance for the configuration scenario shown in [Figure 6-1](#). The procedure uses sample parameters based on the scenario.

This configuration procedure assumes that the adaptive security appliance already has interfaces configured for the inside interface, the outside interface, and the DMZ interface. Set up interfaces on the adaptive security appliance by using the Startup Wizard in ASDM. Be sure that the DMZ interface security level is set between 0 and 100. (A common choice is 50.)

For more information about using the Startup Wizard, see [Chapter 5](#), “Configuring the Adaptive Security Appliance.”

The section includes the following topics:

- [Configuration Requirements, page 6-5](#)
- [Enabling Inside Clients to Communicate with Devices on the Internet, page 6-6](#)
- [Enabling Inside Clients to Communicate with the DMZ Web Server, page 6-6](#)
- [Configuring an External Identity for the DMZ Web Server, page 6-10](#)
- [Providing Public HTTP Access to the DMZ Web Server, page 6-12](#)

The following sections provide detailed instructions for how to perform each step.

Configuration Requirements

Configuring the adaptive security appliance for this DMZ deployment requires the following:

- Internal clients need to be able to communicate with devices on the Internet.
- Internal clients need to be able to communicate with the DMZ web server.

- External clients need to be able to communicate with the DMZ web server.

The remainder of this chapter provides instructions for how to complete this configuration.

Enabling Inside Clients to Communicate with Devices on the Internet

To permit internal clients to request content from devices on the Internet, the adaptive security appliance translates the real IP addresses of internal clients to the external address of the outside interface (that is, the public IP address of the adaptive security appliance). Outgoing traffic appears to come from this address.

The ASA 5505 comes with a default configuration that includes the necessary address translation rule. Unless you want to change the IP address of the inside interface, you do not need to configure any settings to allow inside clients to access the Internet.

Enabling Inside Clients to Communicate with the DMZ Web Server

In this procedure, you configure the adaptive security appliance to allow internal clients to communicate securely with the web server in the DMZ. To accomplish this, you must configure a NAT rule between the DMZ and inside interfaces that translates the real IP address of the DMZ web server to its public IP address (10.30.30.30 to 209.165.200.225).

This is necessary because when an internal client sends a DNS lookup request, the DNS server returns the public IP address of the DMZ web server.



Note

Because there is no DNS server on the inside network, DNS requests must exit the adaptive security appliance to be resolved by a DNS server on the Internet.

This section includes the following topics:

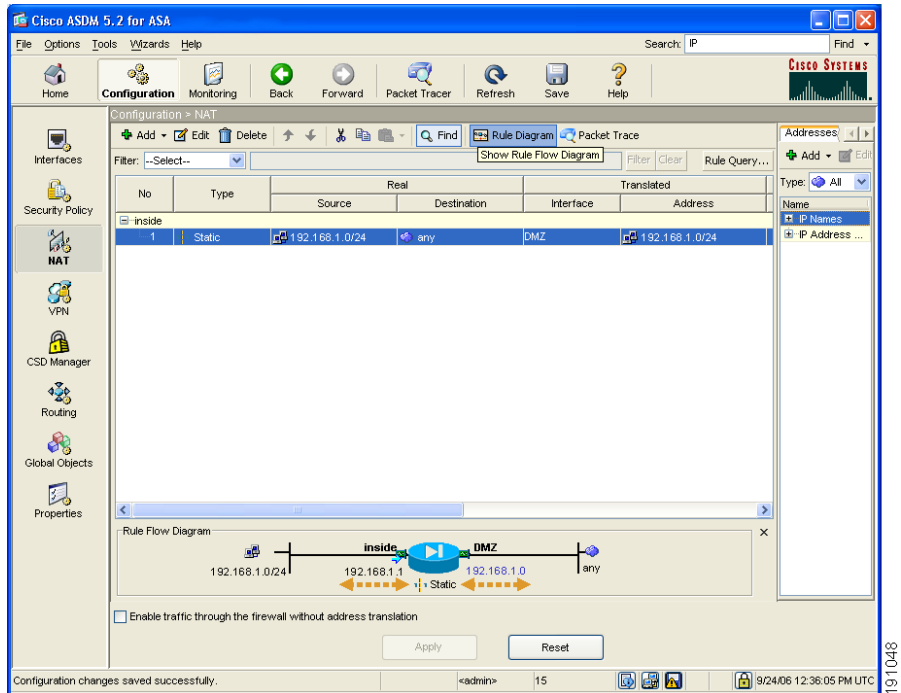
- [Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces, page 6-7](#)

- [Translating the Public Address of the Web Server to its Real Address on the Inside Interface, page 6-8](#)

Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces

To configure NAT to translate internal client IP addresses between the inside interface and the DMZ interface, perform the following steps:

-
- Step 1** In the ASDM main window, click the **Configuration** tool.
 - Step 2** In the Features pane, click **NAT**.
 - Step 3** From the Add drop-down list, choose Add Static NAT Rule.
The Add Static NAT Rule dialog box appears.
 - Step 4** In the Real Address area, specify the IP address to be translated. For this scenario, address translation for inside clients is performed for the entire 192.168.1.0 subnet.
 - a.** From the Interface drop-down list, choose the Inside interface.
 - b.** Enter the IP address of the client or network. In this scenario, the IP address of the network is 192.168.1.0.
 - c.** From the Netmask drop-down list, choose 255.255.255.0 for this scenario.
 - Step 5** In the Static Translation area, do the following:
 - a.** From the Interface drop-down list, choose the DMZ interface.
 - b.** In the IP Address field, enter the IP address of the internal client subnet. In this scenario, the IP address is 192.168.1.0.
 - c.** Click **OK** to add the static NAT rule and return to the Configuration > NAT pane.
 - Step 6** Review the configuration pane to verify that the translation rule appears as you expected. The rule should appear similar to the following:



Step 7 Click **Apply** to complete the adaptive security appliance configuration changes.

Translating the Public Address of the Web Server to its Real Address on the Inside Interface

To configure NAT rule that translates the public IP address of the web server to its real IP address, perform the following steps:

Step 1 In the main ASDM window, choose **Configuration > NAT**.

Step 2 From the Add drop-down list, choose Add Static NAT Rule.

The Add Static NAT Rule dialog box appears.

- Step 3** In the Real Address area, do the following:
- From the Interface drop-down list, choose DMZ.
 - Enter or choose from the IP Address drop-down list the private address of the DMZ web server. In this scenario, the private IP address is **10.30.30.30**.
- Step 4** In the Static Translation area, do the following:
- From the Interface drop-down list, choose Inside.
 - Enter or choose from the IP Address drop-down list the public address of the DMZ web server. In this scenario, the public IP address is **209.165.200.226**.

Add Static NAT Rule

Real Address

Interface: dmz

IP Address: 10.30.30.30

Netmask: 255.255.255.255

Static Translation

Interface: inside

IP Address: 209.165.200.226

Enable Port Address Translation (PAT)

Protocol: TCP

Original Port:

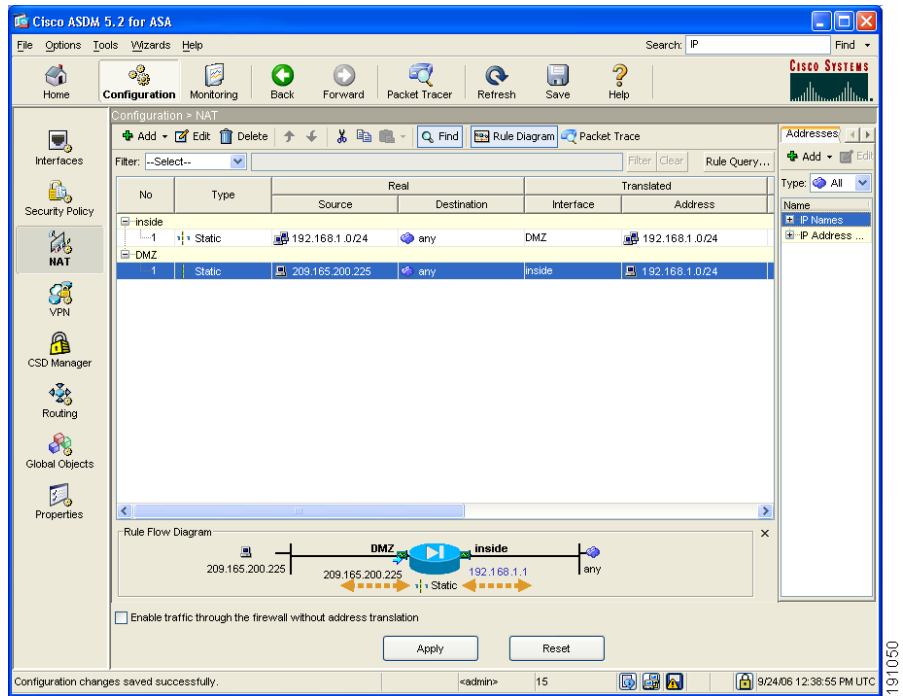
Translated Port:

NAT Options...

OK Cancel Help

Configuring the Security Appliance for a DMZ Deployment

- Step 5** Click **OK** to return to the Configuration > NAT pane. The configuration should look similar to the following:



Configuring an External Identity for the DMZ Web Server

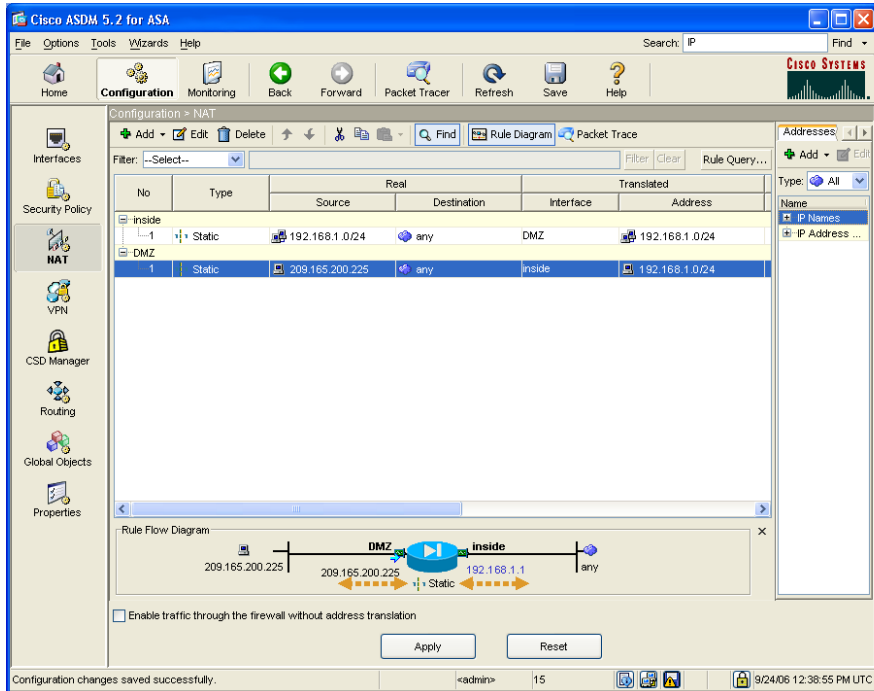
The DMZ web server needs to be accessible by all hosts on the Internet. This configuration requires translating the private IP address of the DMZ web server to a public IP address, which allows outside HTTP clients to access the web server without being aware of the adaptive security appliance. To map the real web server IP address (10.30.30.30) statically to a public IP address (209.165.200.226), perform the following steps:

- Step 1** In the ASDM main window, choose **Configuration > NAT**.

- Step 2** From the Add drop-down list, choose Add Static NAT Rule.
The Add Static NAT Rule dialog box appears.
- Step 3** In the Real Address area, specify the following:
- From the Interface drop-down list, choose the DMZ interface.
 - Enter the real IP address of the DMZ web server. In this scenario, the IP address is **10.30.30.30**.
 - From the Netmask drop-down list, choose 255.255.255.255.
- Step 4** In the Static Translation area, specify the public IP address to be used for the web server:
- From the Interface drop-down list, choose Outside.
 - From the IP Address drop-down list, choose the Interface IP keyword, which is the IP address for the specified outside interface, in this case.
- Step 5** Configure Port Address Translation.
- Because there is only one public IP address, it is necessary to use Port Address Translation to translate the IP address of the DMZ web server to the public outside IP address of the adaptive security appliance. To configure Port Address Translation, perform the following steps:
- Check the **Enable Port Address Translation (PAT)** check box.
 - From the Protocol drop-down list, choose tcp.
 - In the Original Port field, enter **80**.
 - In the Translated Port field, enter **80**.
 - Click **OK** to add the rule and return to the list of Address Translation Rules.
- This rule maps the real web server IP address (10.30.30.30) statically to the public IP address of the web server (209.165.200.225).

Configuring the Security Appliance for a DMZ Deployment

- Step 6** Confirm that the rule was created the way you expected. The displayed configuration should be similar to the following:



- Step 7** Click **Apply** to complete the adaptive security appliance configuration changes.

Providing Public HTTP Access to the DMZ Web Server

By default, the adaptive security appliance denies all traffic coming in from the public network. To permit traffic coming from the Internet to access the DMZ web server, you must configure an access control rule permitting incoming HTTP traffic destined for the DMZ web server.

This access control rule specifies the interface of the adaptive security appliance that processes the traffic, that the traffic is incoming, the origin and destination of the traffic, and the type of traffic protocol and service to be permitted.

In this section, you create an access rule that permits incoming HTTP traffic originating from any host or network on the Internet, if the destination of the traffic is the web server on the DMZ network. All other traffic coming in from the public network is denied.

To configure the access control rule, perform the following steps:

-
- Step 1** In the ASDM main window, do the following:
- Choose **Configuration > Security Policy**.
 - Click the **Access Rules** tab, then from the Add pull-down list, choose Add Access Rule.
The Add Access Rule dialog box appears.
- Step 2** In the Interface and Action area, do the following:
- From the Interface drop-down list, choose Outside.
 - From the Direction drop-down list, choose Incoming.
 - From the Action drop-down list, choose Permit.
- Step 3** In the Source area, choose the Any keyword from the Type drop-down list to allow traffic originating from any host or network.
- Step 4** In the Destination area, do the following:
- From the Type drop-down list, choose the Interface IP keyword.
 - From the Interface drop-down list, choose Outside.
- Step 5** In the Protocol and Service area, specify the type of traffic that you want to permit through the adaptive security appliance.
- From the Protocol drop-down list, choose tcp.
 - In the Source Port area, confirm that the Service radio button is set to “=” (equal to), and then choose Any from the next drop-down list.
 - In the Destination Port area, confirm that the Service radio button is set to “=” (equal to), and then choose HTTP/WWW from the next drop-down list.
- At this point, the entries in the Add Access Rule dialog box should be similar to the following:

Add Access Rule

Interface and Action
 Interface: outside
 Direction: incoming
 Action: Permit

Source
 Type: any

Destination
 Type: Interface IP

Protocol and Service
 Protocol: tcp
 Source Port: Service: = any
 Destination Port: Service: = any

Rule Flow Diagram
 any — outside — 209.165.200.225
 Permit

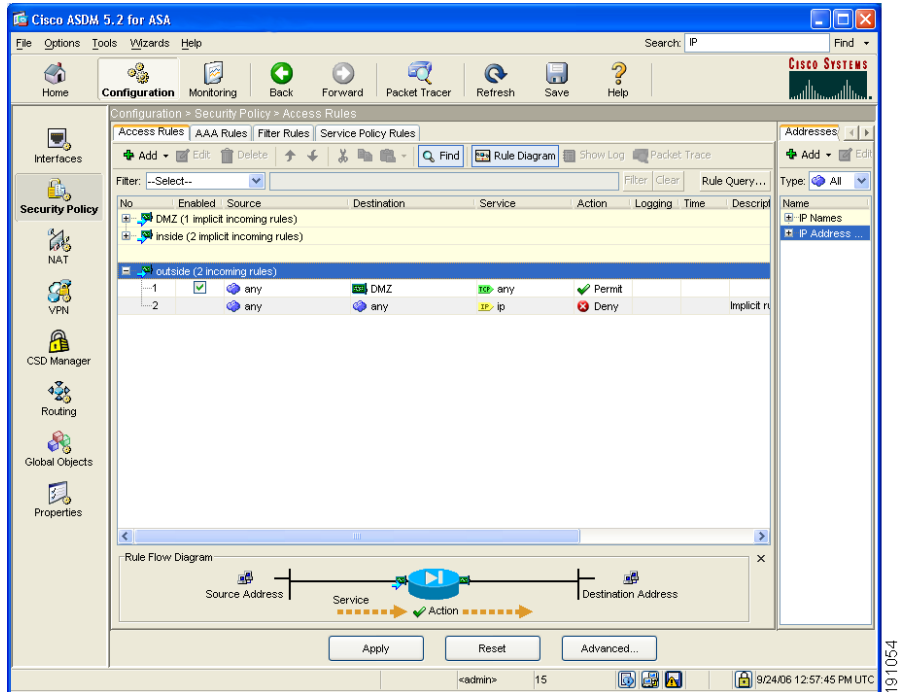
Options
 Logging: Default Syslog Level: Informational Log Interval: 300
 Time Range: (any)
 Description:

OK Cancel Help

191053

d. Click **OK** to return to the Security Policy > Access Rules pane.

Step 6 The displayed configuration should be similar to the following. Verify that the information you entered is accurate.



Step 7 Click **Apply** to save the changes to the configuration that the adaptive security appliance is currently running.

With this setting, clients on the public network can resolve HTTP requests for content from the DMZ web server, while keeping the private network secure.

Step 8 If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, choose **Save**.

Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the previous configuration takes effect the next time that the device starts.

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	Cisco Security Appliance Command Line Configuration Guide
Learn about daily operations	Cisco Security Appliance Command Reference Cisco Security Appliance Logging Configuration and System Log Messages

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	Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration”
Configure a site-to-site VPN	Chapter 8, “Scenario: Site-to-Site VPN Configuration”