



CHAPTER 6

Configuring the Transparent or Routed Firewall

This chapter describes how to configure the firewall mode, routed or transparent, and how to customize transparent firewall operation.



Note

In multiple context mode, you cannot set the firewall mode separately for each context; you can only set the firewall mode for the entire security appliance.

This chapter includes the following sections:

- [Configuring the Firewall Mode, page 6-1](#)
- [Configuring ARP Inspection for the Transparent Firewall, page 6-8](#)
- [Customizing the MAC Address Table for the Transparent Firewall, page 6-11](#)
- [Firewall Mode Examples, page 6-14](#)

Configuring the Firewall Mode

This section describes routed and transparent firewall mode, and how to set the mode. This section includes the following topics:

- [Information About the Firewall Mode, page 6-1](#)
- [Licensing Requirements for the Firewall Mode, page 6-4](#)
- [Default Settings, page 6-4](#)
- [Guidelines and Limitations, page 6-5](#)
- [Setting the Firewall Mode, page 6-7](#)
- [Feature History for Firewall Mode, page 6-8](#)

Information About the Firewall Mode

This section describes routed and transparent firewall mode, and includes the following topics:

- [Information About Routed Firewall Mode, page 6-2](#)
- [Information About Transparent Firewall Mode, page 6-2](#)

Information About Routed Firewall Mode

In routed mode, the security appliance is considered to be a router hop in the network. It can use OSPF or RIP (in single context mode). Routed mode supports many interfaces. Each interface is on a different subnet. You can share interfaces between contexts.

The security appliance acts as a router between connected networks, and each interface requires an IP address on a different subnet. In single context mode, the routed firewall supports OSPF and RIP. Multiple context mode supports static routes only. We recommend using the advanced routing capabilities of the upstream and downstream routers instead of relying on the security appliance for extensive routing needs.

Information About Transparent Firewall Mode

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

This section describes transparent firewall mode, and includes the following topics:

- [Transparent Firewall Network, page 6-2](#)
- [Allowing Layer 3 Traffic, page 6-2](#)
- [Allowed MAC Addresses, page 6-2](#)
- [Passing Traffic Not Allowed in Routed Mode, page 6-3](#)
- [BPDU Handling, page 6-3](#)
- [MAC Address vs. Route Lookups, page 6-3](#)
- [Using the Transparent Firewall in Your Network, page 6-4](#)

Transparent Firewall Network

The security appliance connects the same network on its inside and outside interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network.

Allowing Layer 3 Traffic

IPv4 and IPv6 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without an access list. ARPs are allowed through the transparent firewall in both directions without an access list. ARP traffic can be controlled by ARP inspection. For Layer 3 traffic travelling from a low to a high security interface, an extended access list is required on the low security interface. See [Chapter 21, “Configuring Access Rules and ACLs,”](#) for more information.

Allowed MAC Addresses

The following destination MAC addresses are allowed through the transparent firewall. Any MAC address not on this list is dropped.

- TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF
- IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
- IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
- BPDU multicast address equal to 0100.0CCC.CCCD

- Appletalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF

Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. The transparent firewall, however, can allow almost any traffic through using either an extended access list (for IP traffic) or an EtherType access list (for non-IP traffic).

**Note**

The transparent mode security appliance does not pass CDP packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. For example, you cannot pass IS-IS packets. An exception is made for BPDUs, which are supported.

For example, you can establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on an extended access list. Likewise, protocols like HSRP or VRRP can pass through the security appliance.

Non-IP traffic (for example AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through using an EtherType access list.

For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality. For example, by using an extended access list, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV.

BPDUs Handling

To prevent loops using the spanning tree protocol, BPDUs are passed by default. To block BPDUs, you need to configure an EtherType access list to deny them.

MAC Address vs. Route Lookups

When the security appliance runs in transparent mode, the outgoing interface of a packet is determined by performing a MAC address lookup instead of a route lookup.

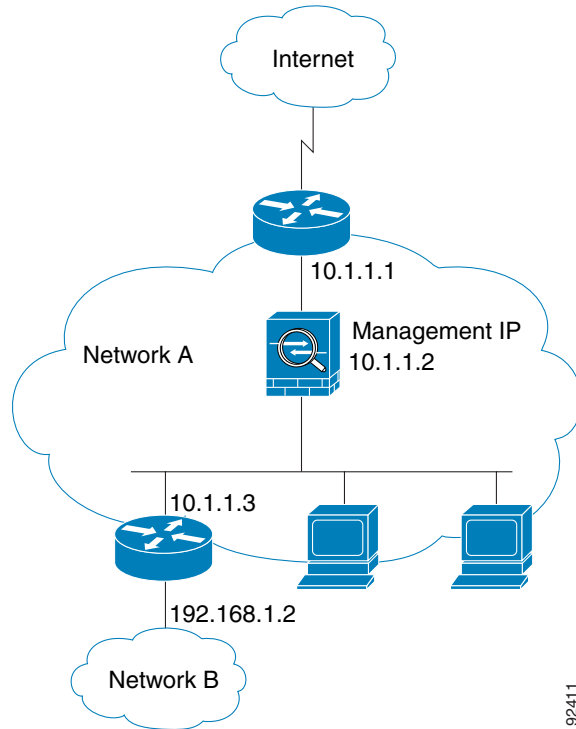
Route lookups, however, are necessary for the following traffic types:

- Traffic originating on the security appliance—For example, if your syslog server is located on a remote network, you must use a static route so the security appliance can reach that subnet.
- Voice over IP (VoIP) traffic with inspection enabled, and the endpoint is at least one hop away from the security appliance—For example, if you use the transparent firewall between a CCM and an H.323 gateway, and there is a router between the transparent firewall and the H.323 gateway, then you need to add a static route on the security appliance for the H.323 gateway for successful call completion.
- VoIP or DNS traffic with NAT and inspection enabled—To successfully translate the IP address inside VoIP and DNS packets, the security appliance needs to perform a route lookup. Unless the host is on a directly-connected network, then you need to add a static route on the security appliance for the real host address that is embedded in the packet.

Using the Transparent Firewall in Your Network

Figure 6-1 shows a typical transparent firewall network where the outside devices are on the same subnet as the inside devices. The inside router and hosts appear to be directly connected to the outside router.

Figure 6-1 Transparent Firewall Network



92411

Licensing Requirements for the Firewall Mode

The following table shows the licensing requirements for this feature.

| Model | License Requirement |
|------------|---------------------|
| All models | Base License. |

Default Settings

The default mode is routed mode.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

- The firewall mode is set for the entire system and all contexts; you cannot set the mode individually for each context.
- For multiple context mode, set the mode in the system execution space.
- When you change modes, the security appliance clears the running configuration because many commands are not supported for both modes. This action removes any contexts from running. If you then re-add a context that has an existing configuration that was created for the wrong mode, the context configuration might not work correctly. Be sure to recreate your context configurations for the correct mode before you re-add them, or add new contexts with new paths for the new configurations.

Transparent Firewall Guidelines

Follow these guidelines when planning your transparent firewall network:

- For IPv4, a management IP address is required for both management traffic and for traffic to pass through the security appliance. For multiple context mode, an IP address is required for each context.

Unlike routed mode, which requires an IP address for each interface, a transparent firewall has an IP address assigned to the entire device. The security appliance uses this IP address as the source address for packets originating on the security appliance, such as system messages or AAA communications.

The management IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255).

For IPv6, at a minimum you need to configure link-local addresses for each interface for through traffic. For full functionality, including the ability to manage the security appliance, you need to configure a global IP address for the device.

You can configure an IP address (both IPv4 and IPv6) for the Management 0/0 or Management 0/1 management-only interface. This IP address can be on a separate subnet from the main management IP address.

- The transparent security appliance uses an inside interface and an outside interface only. If your platform includes a dedicated management interface, you can also configure the management interface or subinterface for management traffic only.



Note In transparent firewall mode, the management interface updates the MAC address table in the same manner as a data interface; therefore you should not connect both a management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Cisco Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the management interface from the physically-connected switch, then the security appliance updates the MAC address table to use the *management* interface to access the switch, instead of the data interface. This action causes a temporary traffic interruption; the security appliance will not re-update the MAC address table for packets from the switch to the data interface for at least 30 seconds for security reasons.

In single mode, you can only use two data interfaces (and the dedicated management interface, if available) even if your security appliance includes more than two interfaces.

- Each directly connected network must be on the same subnet.
- Do not specify the security appliance management IP address as the default gateway for connected devices; devices need to specify the router on the other side of the security appliance as the default gateway.
- For multiple context mode, each context must use different interfaces; you cannot share an interface across contexts.
- For multiple context mode, each context typically uses a different subnet. You can use overlapping subnets, but your network topology requires router and NAT configuration to make it possible from a routing standpoint.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines and Limitations

- When you change modes, the security appliance clears the running configuration because many commands are not supported for both modes. The startup configuration remains unchanged. If you reload without saving, then the startup configuration is loaded, and the mode reverts back to the original setting. See the [“Setting the Firewall Mode” section on page 6-7](#) for information about backing up your configuration file.
- If you download a text configuration to the security appliance that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the security appliance changes the mode as soon as it reads the command and then continues reading the configuration you downloaded. If the command appears later in the configuration, the security appliance clears all the preceding lines in the configuration.

Unsupported Features in Transparent Mode

[Table 6-1](#) lists the features are not supported in transparent mode.

Table 6-1 *Unsupported Features in Transparent Mode*

| Feature | Description |
|---------------------------|--|
| Dynamic DNS | — |
| DHCP relay | The transparent firewall can act as a DHCP server, but it does not support the DHCP relay commands. DHCP relay is not required because you can allow DHCP traffic to pass through using two extended access lists: one that allows DHCP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction. |
| Dynamic routing protocols | You can, however, add static routes for traffic originating on the security appliance. You can also allow dynamic routing protocols through the security appliance using an extended access list. |
| Multicast IP routing | You can allow multicast traffic through the security appliance by allowing it in an extended access list. |

Table 6-1 *Unsupported Features in Transparent Mode*

| Feature | Description |
|-------------------------------------|---|
| QoS | — |
| VPN termination for through traffic | The transparent firewall supports site-to-site VPN tunnels for management connections only. It does not terminate VPN connections for traffic through the security appliance. You can pass VPN traffic through the security appliance using an extended access list, but it does not terminate non-management connections. SSL VPN is also not supported. |

Setting the Firewall Mode

This section describes how to change the firewall mode using the CLI. You cannot change the mode in ASDM.



Note

We recommend that you set the firewall mode before you perform any other configuration because changing the firewall mode clears the running configuration.

Prerequisites

When you change modes, the security appliance clears the running configuration (see the “[Guidelines and Limitations](#)” section on page 6-5 for more information).

- If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.
- Use the CLI at the console port to change the mode. If you use any other type of session, including the ASDM Command Line Interface tool or SSH, you will be disconnected when the configuration is cleared, and you will have to reconnect to the security appliance using the console port in any case.

Detailed Steps

| Command | Purpose |
|--|--|
| firewall transparent Example: hostname(config)# firewall transparent | Sets the firewall mode to transparent. Enter this command in the system execution space for multiple context mode. To change the mode to routed, enter the no firewall transparent command. This command also appears in each context configuration for informational purposes only; you cannot enter this command in a context. Note You are not prompted to confirm the firewall mode change; the change occurs immediately. |

Feature History for Firewall Mode

Table 6-2 lists the release history for this feature.

Table 6-2 Feature History for Firewall Mode

| Feature Name | Releases | Feature Information |
|---------------------------|----------|--|
| Transparent firewall mode | 7.0(1) | A transparent firewall is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. The following commands were introduced: firewall transparent , show firewall . |

Configuring ARP Inspection for the Transparent Firewall

This section describes ARP inspection and how to enable it, and includes the following topics:

- [Information About ARP Inspection, page 6-8](#)
- [Licensing Requirements for ARP Inspection, page 6-9](#)
- [Default Settings, page 6-9](#)
- [Guidelines and Limitations, page 6-9](#)
- [Configuring ARP Inspection, page 6-9](#)
- [Feature History for ARP Inspection, page 6-11](#)

Information About ARP Inspection

By default, all ARP packets are allowed through the security appliance. You can control the flow of ARP packets by enabling ARP inspection.

When you enable ARP inspection, the security appliance compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the security appliance to either forward the packet out all interfaces (flood), or to drop the packet.



Note

The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address.

The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

Licensing Requirements for ARP Inspection

The following table shows the licensing requirements for this feature.

| Model | License Requirement |
|------------|---------------------|
| All models | Base License. |

Default Settings

By default, all ARP packets are allowed through the security appliance.

If you enable ARP inspection, the default setting is to flood non-matching packets.

Guidelines and Limitations

Context Mode Guidelines

- Supported in single and multiple context mode.
- In multiple context mode, configure ARP inspection within each context.

Firewall Mode Guidelines

Supported only in transparent firewall mode. Routed mode is not supported.

Configuring ARP Inspection

This section describes how to configure ARP inspection, and includes the following topics:

- [Task Flow for Configuring ARP Inspection, page 6-9](#)
- [Adding a Static ARP Entry, page 6-10](#)
- [Enabling ARP Inspection, page 6-10](#)

Task Flow for Configuring ARP Inspection

Follow these steps to configure ARP Inspection:

- Step 1** Add static ARP entries according to the [“Adding a Static ARP Entry” section on page 6-10](#). ARP inspection compares ARP packets with static ARP entries in the ARP table, so static ARP entries are required for this feature.

- Step 2** Enable ARP inspection according to the [“Enabling ARP Inspection”](#) section on page 6-10.
-

Adding a Static ARP Entry

ARP inspection compares ARP packets with static ARP entries in the ARP table. Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver. The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.



Note

The transparent firewall uses dynamic ARP entries in the ARP table for traffic to and from the security appliance, such as management traffic.

Detailed Steps

- Step 1** Choose the **Configuration > Device Setup > ARP > ARP Static Table** pane.
- Step 2** (Optional) To set the ARP timeout for *dynamic* ARP entries, enter a value in the ARP Timeout field.
This field sets the amount of time before the security appliance rebuilds the ARP table, between 60 to 4294967 seconds. The default is 14400 seconds. Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently.
- Step 3** Click **Add**.
The Add ARP Static Configuration dialog box appears.
- Step 4** From the Interface drop-down list, choose the interface attached to the host network.
- Step 5** In the IP Address field, enter the IP address of the host.
- Step 6** In the MAC Address field, enter the MAC address of the host; for example, 00e0.1e4e.3d8b.
- Step 7** To perform proxy ARP for this address, check the **Proxy ARP** check box.
If the security appliance receives an ARP request for the specified IP address, then it responds with the specified MAC address.
- Step 8** Click **OK**, and then **Apply**.
-


What to Do Next

Enable ARP inspection according to the [“Enabling ARP Inspection”](#) section on page 6-10.

Enabling ARP Inspection

This section describes how to enable ARP inspection.

Detailed Steps

-
- Step 1** Choose the **Configuration > Device Setup > ARP > ARP Inspection** pane.
- Step 2** Choose the interface row on which you want to enable ARP inspection, and click **Edit**.
The Edit ARP Inspection dialog box appears.
- Step 3** To enable ARP inspection, check the **Enable ARP Inspection** check box.
- Step 4** (Optional) To flood non-matching ARP packets, check the **Flood ARP Packets** check box.
By default, packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet.
If you uncheck this check box, all non-matching packets are dropped, which restricts ARP through the security appliance to only static entries.
-  **Note** The Management 0/0 or 0/1 interface or subinterface, if present, never floods packets even if this parameter is set to flood.
-
- Step 5** Click **OK**, and then **Apply**.
-

Feature History for ARP Inspection

Table 6-2 lists the release history for this feature.

Table 6-3 Feature History for ARP Inspection

| Feature Name | Releases | Feature Information |
|----------------|----------|---|
| ARP inspection | 7.0(1) | ARP inspection compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table. The following commands were introduced: arp , arp-inspection , and show arp-inspection . |

Customizing the MAC Address Table for the Transparent Firewall

This section describes the MAC address table, and includes the following topics:

- [Information About the MAC Address Table, page 6-12](#)
- [Licensing Requirements for ARP Inspection, page 6-12](#)
- [Default Settings, page 6-12](#)
- [Guidelines and Limitations, page 6-12](#)
- [Configuring the MAC Address Table, page 6-13](#)

- [Feature History for the MAC Address Table, page 6-14](#)

Information About the MAC Address Table

The security appliance learns and builds a MAC address table in a similar way as a normal bridge or switch: when a device sends a packet through the security appliance, the security appliance adds the MAC address to its table. The table associates the MAC address with the source interface so that the security appliance knows to send any packets addressed to the device out the correct interface.

The ASA 5505 adaptive security appliance includes a built-in switch; the switch MAC address table maintains the MAC address-to-switch port mapping for traffic within each VLAN. This section discusses the bridge MAC address table, which maintains the MAC address-to-VLAN interface mapping for traffic that passes between VLANs.

Because the security appliance is a firewall, if the destination MAC address of a packet is not in the table, the security appliance does not flood the original packet on all interfaces as a normal bridge does. Instead, it generates the following packets for directly connected devices or for remote devices:

- Packets for directly connected devices—The security appliance generates an ARP request for the destination IP address, so that the security appliance can learn which interface receives the ARP response.
- Packets for remote devices—The security appliance generates a ping to the destination IP address so that the security appliance can learn which interface receives the ping reply.

The original packet is dropped.

Licensing Requirements for ARP Inspection

The following table shows the licensing requirements for this feature.

| Model | License Requirement |
|------------|---------------------|
| All models | Base License. |

Default Settings

The default timeout value for dynamic MAC address table entries is 5 minutes.

By default, each interface automatically learns the MAC addresses of entering traffic, and the security appliance adds corresponding entries to the MAC address table.

Guidelines and Limitations

Context Mode Guidelines

- Supported in single and multiple context mode.
- In multiple context mode, configure the MAC address table within each context.

Firewall Mode Guidelines

Supported only in transparent firewall mode. Routed mode is not supported.

Additional Guidelines

In transparent firewall mode, the management interface updates the MAC address table in the same manner as a data interface; therefore you should not connect both a management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Cisco Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the management interface from the physically-connected switch, then the security appliance updates the MAC address table to use the *management* interface to access the switch, instead of the data interface. This action causes a temporary traffic interruption; the security appliance will not re-update the MAC address table for packets from the switch to the data interface for at least 30 seconds for security reasons.

Configuring the MAC Address Table

This section describes how you can customize the MAC address table, and includes the following sections:

- [Adding a Static MAC Address, page 6-13](#)
- [Disabling MAC Address Learning, page 6-13](#)

Adding a Static MAC Address

Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the security appliance drops the traffic and generates a system message. When you add a static ARP entry (see the [“Adding a Static ARP Entry” section on page 6-10](#)), a static MAC address entry is automatically added to the MAC address table.

To add a static MAC address to the MAC address table, perform the following steps:

-
- Step 1** Choose the **Configuration > Device Setup > Bridging > MAC Address Table** pane.
 - Step 2** (Optional) To set the time a MAC address entry stays in the MAC address table before timing out, enter a value in the Dynamic Entry Timeout field.
This value is between 5 and 720 minutes (12 hours). 5 minutes is the default.
 - Step 3** Click **Add**.
The Add MAC Address Entry dialog box appears.
 - Step 4** From the Interface Name drop-down list, choose the source interface associated with the MAC address.
 - Step 5** In the MAC Address field, enter the MAC address.
 - Step 6** Click **OK**, and then **Apply**.
-

Disabling MAC Address Learning

By default, each interface automatically learns the MAC addresses of entering traffic, and the security appliance adds corresponding entries to the MAC address table. You can disable MAC address learning if desired, however, unless you statically add MAC addresses to the table, no traffic can pass through the security appliance.

To disable MAC address learning, perform the following steps:

-
- Step 1** Choose the **Configuration > Device Setup > Bridging > MAC Learning** pane.
 - Step 2** To disable MAC learning, choose an interface row, and click **Disable**.
 - Step 3** To reenable MAC learning, click **Enable**.
 - Step 4** Click **Apply**.
-

Feature History for the MAC Address Table

Table 6-2 lists the release history for this feature.

Table 6-4 Feature History for the MAC Address Table

| Feature Name | Releases | Feature Information |
|-------------------|----------|---|
| MAC address table | 7.0(1) | Transparent firewall mode uses a MAC address table. The following commands were introduced: mac-address-table static , mac-address-table aging-time , mac-learn disable , and show mac-address-table . |

Firewall Mode Examples

This section includes examples of how traffic moves through the security appliance, and includes the following topics:

- [How Data Moves Through the Security Appliance in Routed Firewall Mode, page 6-14](#)
- [How Data Moves Through the Transparent Firewall, page 6-20](#)

How Data Moves Through the Security Appliance in Routed Firewall Mode

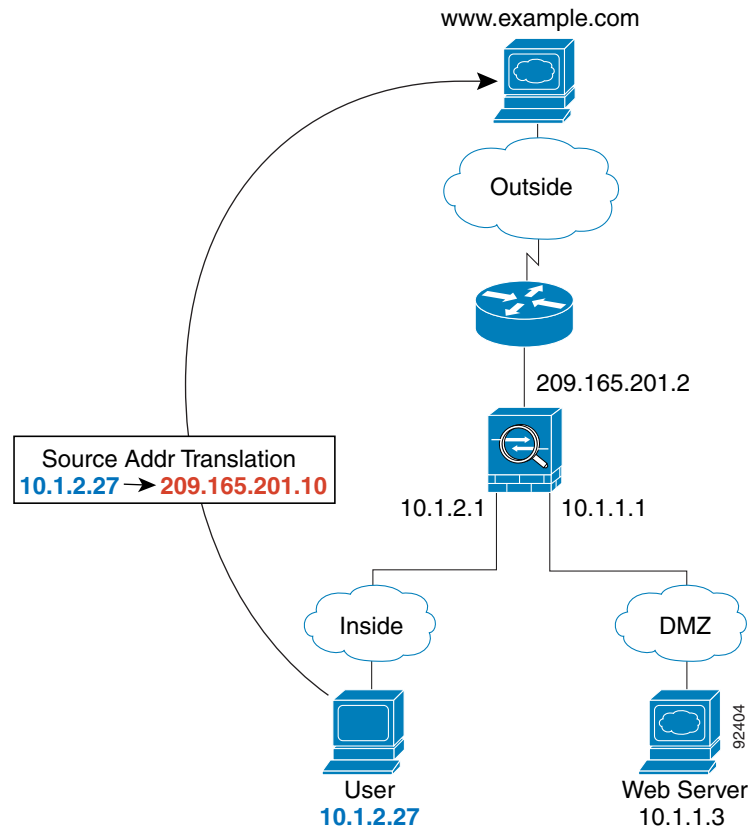
This section describes how data moves through the security appliance in routed firewall mode, and includes the following topics:

- [An Inside User Visits a Web Server, page 6-15](#)
- [An Outside User Visits a Web Server on the DMZ, page 6-16](#)
- [An Inside User Visits a Web Server on the DMZ, page 6-17](#)
- [An Outside User Attempts to Access an Inside Host, page 6-18](#)
- [A DMZ User Attempts to Access an Inside Host, page 6-19](#)

An Inside User Visits a Web Server

Figure 6-2 shows an inside user accessing an outside web server.

Figure 6-2 Inside to Outside



The following steps describe how data moves through the security appliance (see Figure 6-2):

1. The user on the inside network requests a web page from www.example.com.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the security appliance first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the interface would be unique; the www.example.com IP address does not have a current address translation in a context.

3. The security appliance translates the local source address (10.1.2.27) to the global address 209.165.201.10, which is on the outside interface subnet.

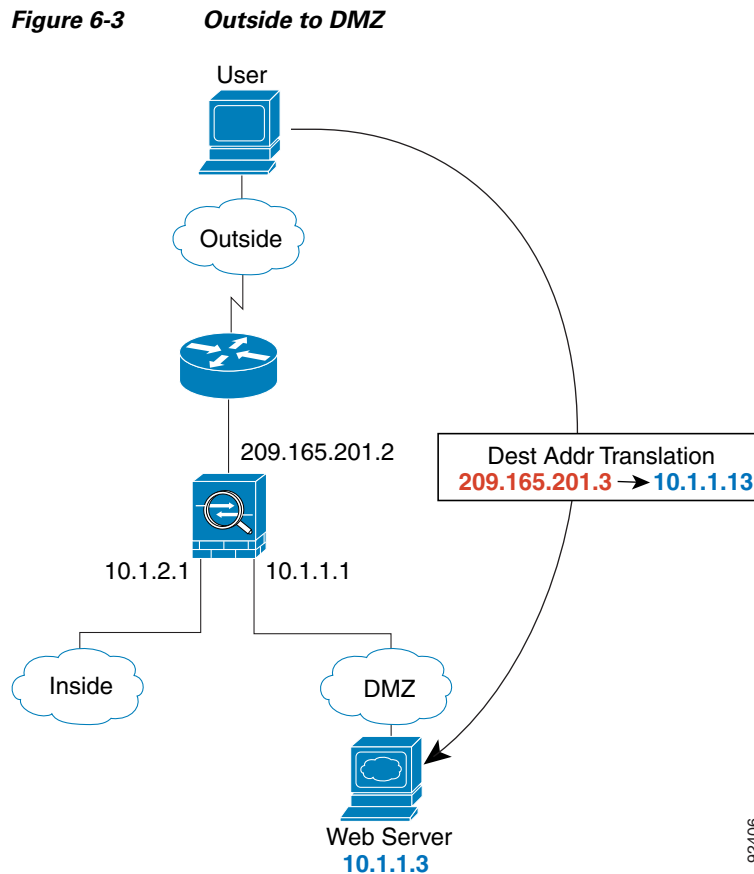
The global address could be on any subnet, but routing is simplified when it is on the outside interface subnet.

4. The security appliance then records that a session is established and forwards the packet from the outside interface.

5. When `www.example.com` responds to the request, the packet goes through the security appliance, and because the session is already established, the packet bypasses the many lookups associated with a new connection. The security appliance performs NAT by translating the global destination address to the local user address, `10.1.2.27`.
6. The security appliance forwards the packet to the inside user.

An Outside User Visits a Web Server on the DMZ

Figure 6-3 shows an outside user accessing the DMZ web server.



The following steps describe how data moves through the security appliance (see Figure 6-3):

1. A user on the outside network requests a web page from the DMZ web server using the global destination address of `209.165.201.3`, which is on the outside interface subnet.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the security appliance first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the classifier “knows” that the DMZ web server address belongs to a certain context because of the server address translation.

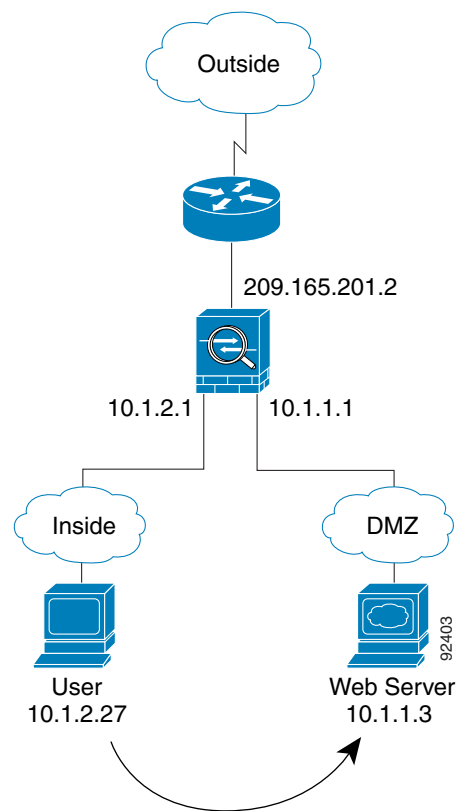
3. The security appliance translates the destination address to the local address `10.1.1.3`.

4. The security appliance then adds a session entry to the fast path and forwards the packet from the DMZ interface.
5. When the DMZ web server responds to the request, the packet goes through the security appliance and because the session is already established, the packet bypasses the many lookups associated with a new connection. The security appliance performs NAT by translating the local source address to 209.165.201.3.
6. The security appliance forwards the packet to the outside user.

An Inside User Visits a Web Server on the DMZ

Figure 6-4 shows an inside user accessing the DMZ web server.

Figure 6-4 Inside to DMZ



The following steps describe how data moves through the security appliance (see Figure 6-4):

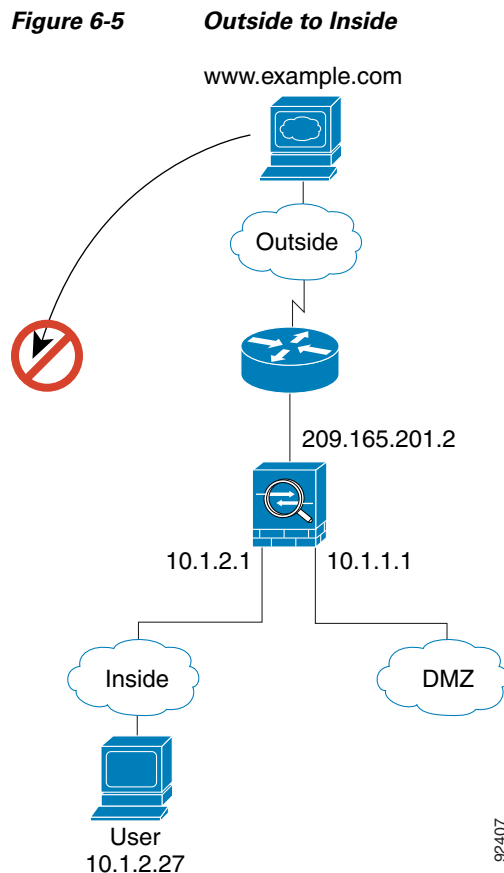
1. A user on the inside network requests a web page from the DMZ web server using the destination address of 10.1.1.3.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the security appliance first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the interface is unique; the web server IP address does not have a current address translation.

3. The security appliance then records that a session is established and forwards the packet out of the DMZ interface.
4. When the DMZ web server responds to the request, the packet goes through the fast path, which lets the packet bypass the many lookups associated with a new connection.
5. The security appliance forwards the packet to the inside user.

An Outside User Attempts to Access an Inside Host

Figure 6-5 shows an outside user attempting to access the inside network.



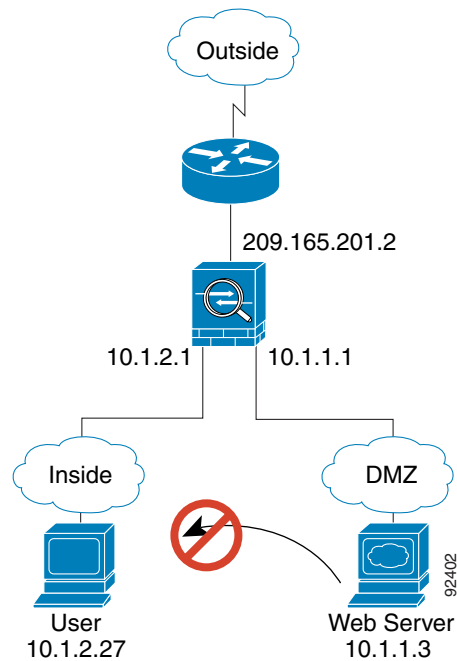
The following steps describe how data moves through the security appliance (see Figure 6-5):

1. A user on the outside network attempts to reach an inside host (assuming the host has a routable IP address).
If the inside network uses private addresses, no outside user can reach the inside network without NAT. The outside user might attempt to reach an inside user by using an existing NAT session.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies if the packet is allowed according to the security policy (access lists, filters, AAA).
3. The packet is denied, and the security appliance drops the packet and logs the connection attempt.
If the outside user is attempting to attack the inside network, the security appliance employs many technologies to determine if a packet is valid for an already established session.

A DMZ User Attempts to Access an Inside Host

Figure 6-6 shows a user in the DMZ attempting to access the inside network.

Figure 6-6 DMZ to Inside



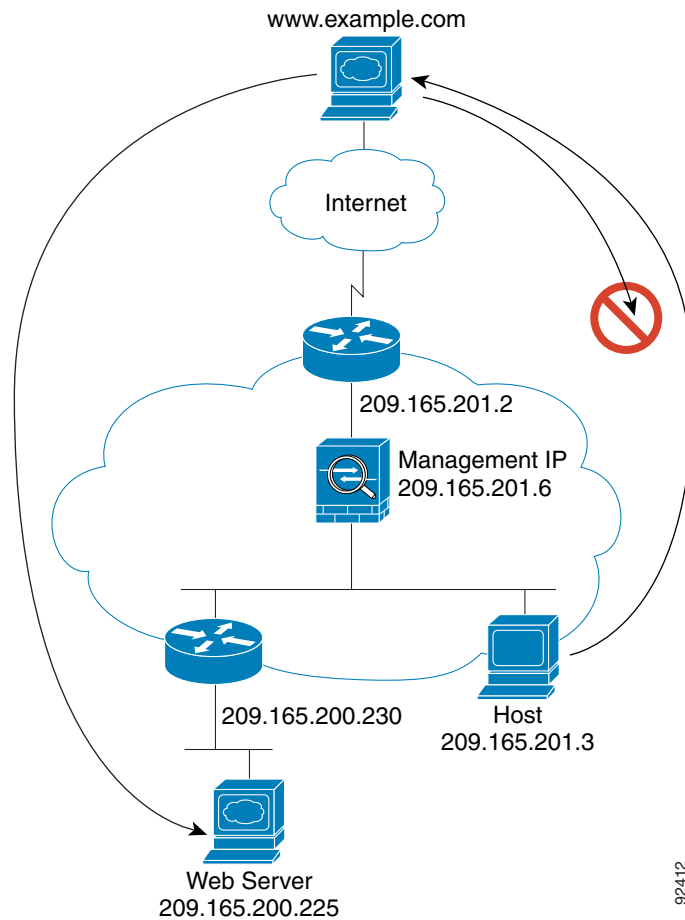
The following steps describe how data moves through the security appliance (see Figure 6-6):

1. A user on the DMZ network attempts to reach an inside host. Because the DMZ does not have to route the traffic on the Internet, the private addressing scheme does not prevent routing.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies if the packet is allowed according to the security policy (access lists, filters, AAA).
The packet is denied, and the security appliance drops the packet and logs the connection attempt.

How Data Moves Through the Transparent Firewall

Figure 6-7 shows a typical transparent firewall implementation with an inside network that contains a public web server. The security appliance has an access list so that the inside users can access Internet resources. Another access list lets the outside users access only the web server on the inside network.

Figure 6-7 Typical Transparent Firewall Data Path



This section describes how data moves through the security appliance, and includes the following topics:

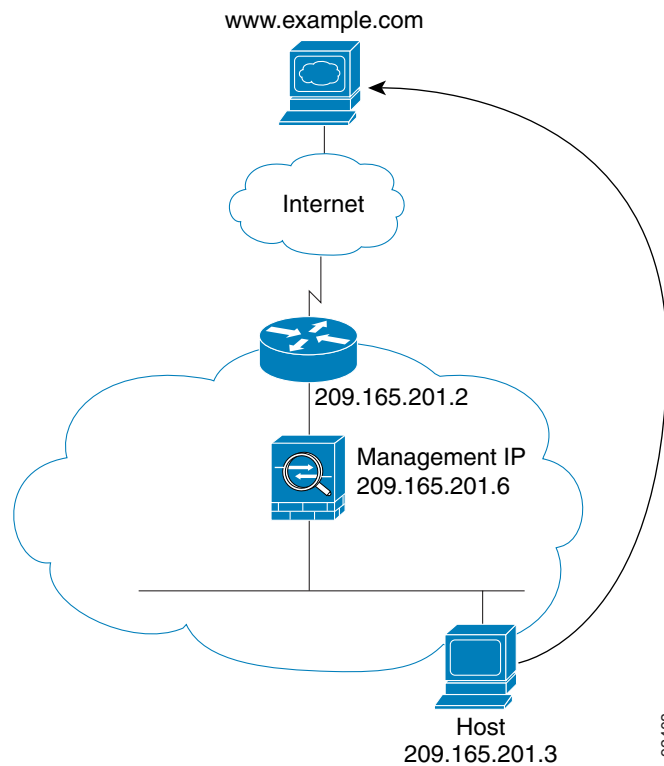
- [An Inside User Visits a Web Server, page 6-21](#)
- [An Inside User Visits a Web Server Using NAT, page 6-22](#)
- [An Outside User Visits a Web Server on the Inside Network, page 6-23](#)
- [An Outside User Attempts to Access an Inside Host, page 6-24](#)

92412

An Inside User Visits a Web Server

Figure 6-8 shows an inside user accessing an outside web server.

Figure 6-8 *Inside to Outside*



The following steps describe how data moves through the security appliance (see Figure 6-8):

1. The user on the inside network requests a web page from www.example.com.
2. The security appliance receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the security appliance first classifies the packet according to a unique interface.

3. The security appliance records that a session is established.
4. If the destination MAC address is in its table, the security appliance forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 209.165.201.2.

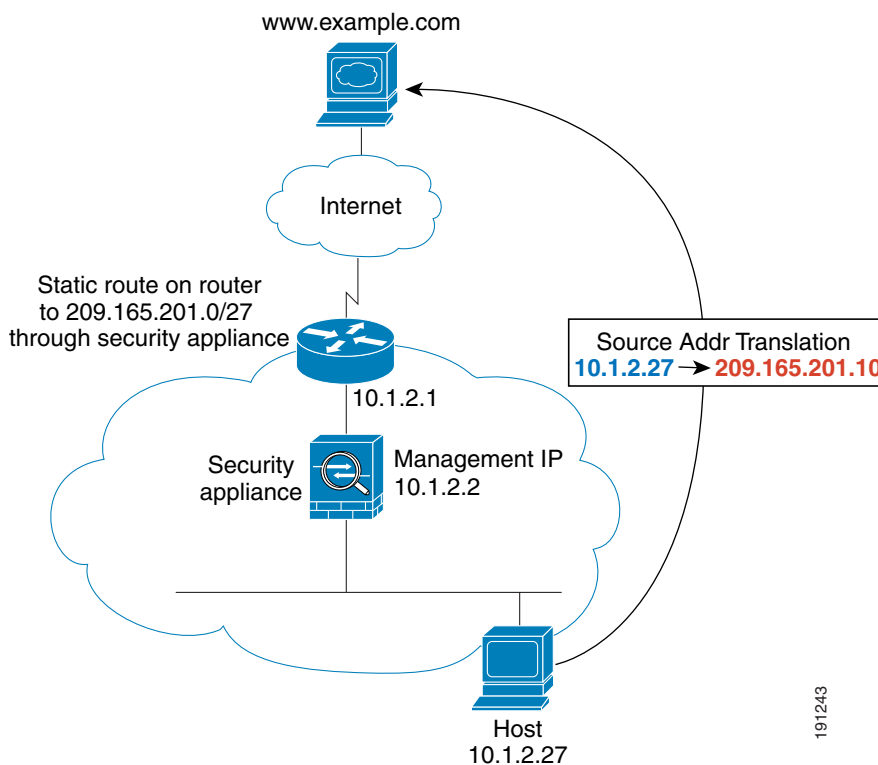
If the destination MAC address is not in the security appliance table, the security appliance attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.

5. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.
6. The security appliance forwards the packet to the inside user.

An Inside User Visits a Web Server Using NAT

Figure 6-8 shows an inside user accessing an outside web server.

Figure 6-9 *Inside to Outside with NAT*



The following steps describe how data moves through the security appliance (see Figure 6-8):

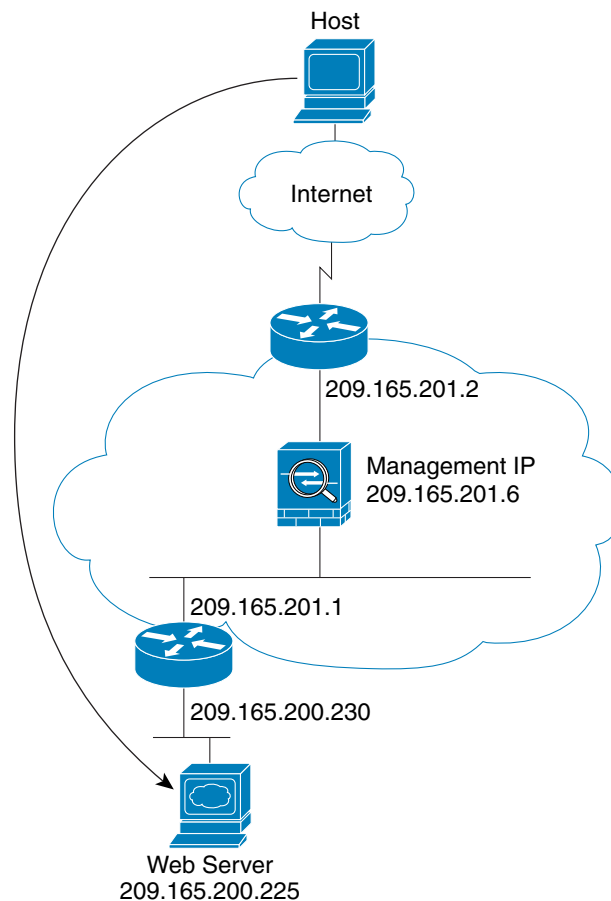
1. The user on the inside network requests a web page from `www.example.com`.
2. The security appliance receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).
For multiple context mode, the security appliance first classifies the packet according to a unique interface.
3. The security appliance translates the real address (10.1.2.27) to the mapped address 209.165.201.10. Because the mapped address is not on the same network as the outside interface, then be sure the upstream router has a static route to the mapped network that points to the security appliance.
4. The security appliance then records that a session is established and forwards the packet from the outside interface.
5. If the destination MAC address is in its table, the security appliance forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 10.1.2.1.
If the destination MAC address is not in the security appliance table, the security appliance attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.
6. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.

- The security appliance performs NAT by translating the mapped address to the real address, 10.1.2.27.

An Outside User Visits a Web Server on the Inside Network

Figure 6-10 shows an outside user accessing the inside web server.

Figure 6-10 Outside to Inside



The following steps describe how data moves through the security appliance (see Figure 6-10):

- A user on the outside network requests a web page from the inside web server.
- The security appliance receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the security appliance first classifies the packet according to a unique interface.

- The security appliance records that a session is established.
- If the destination MAC address is in its table, the security appliance forwards the packet out of the inside interface. The destination MAC address is that of the downstream router, 209.165.201.1.

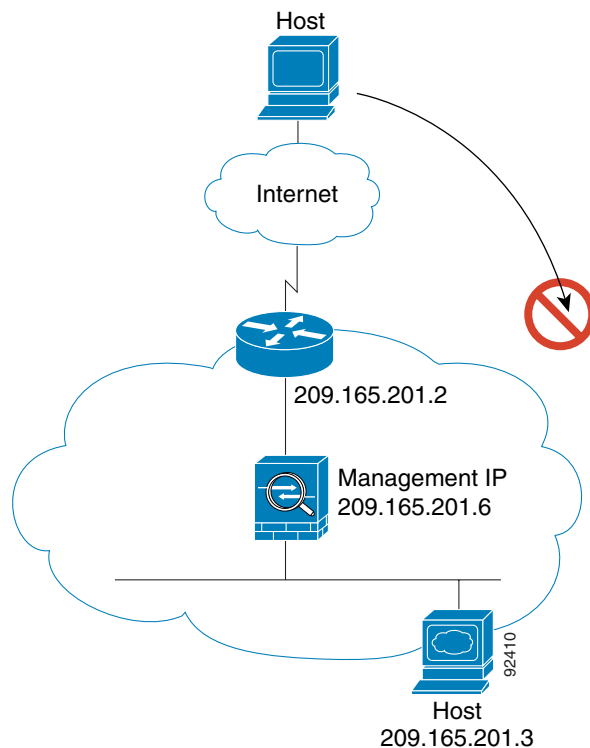
If the destination MAC address is not in the security appliance table, the security appliance attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.

5. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.
6. The security appliance forwards the packet to the outside user.

An Outside User Attempts to Access an Inside Host

Figure 6-11 shows an outside user attempting to access a host on the inside network.

Figure 6-11 Outside to Inside



The following steps describe how data moves through the security appliance (see Figure 6-11):

1. A user on the outside network attempts to reach an inside host.
2. The security appliance receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies if the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the security appliance first classifies the packet according to a unique interface.

3. The packet is denied because there is no access list permitting the outside host, and the security appliance drops the packet.
4. If the outside user is attempting to attack the inside network, the security appliance employs many technologies to determine if a packet is valid for an already established session.