CHAPTER 12

Firewall Mode Overview

This chapter describes how the firewall works in each firewall mode.

The security appliance can run in two firewall modes:

- Routed mode
- Transparent mode

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

In transparent mode, the security appliance acts like a "bump in the wire," or a "stealth firewall," and is not a router hop. The security appliance connects the same network on its inside and outside interfaces. No dynamic routing protocols or NAT are used. However, like routed mode, transparent mode also requires access lists to allow any traffic through the security appliance, except for ARP packets, which are allowed automatically. Transparent mode can allow certain types of traffic in an access list that are blocked by routed mode, including unsupported routing protocols. Transparent mode can also optionally use EtherType access lists to allow non-IP traffic. Transparent mode only supports two interfaces, an inside interface and an outside interface, in addition to a dedicated management interface, if available for your platform.

Note The transparent firewall requires a management IP address. The security appliance uses this IP address as the source address for packets originating on the security appliance. The management IP address must be on the same subnet as the connected network.

This chapter includes the following sections:

Routed Mode Overview

IP Routing Support

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 (in passive mode). 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.

Network Address Translation

NAT substitutes the local address on a packet with a global address that is routable on the destination network. By default, NAT is not required. If you want to enforce a NAT policy that requires hosts on a higher security interface (inside) to use NAT when communicating with a lower security interface (outside), you can enable NAT control (see the **nat-control** command).

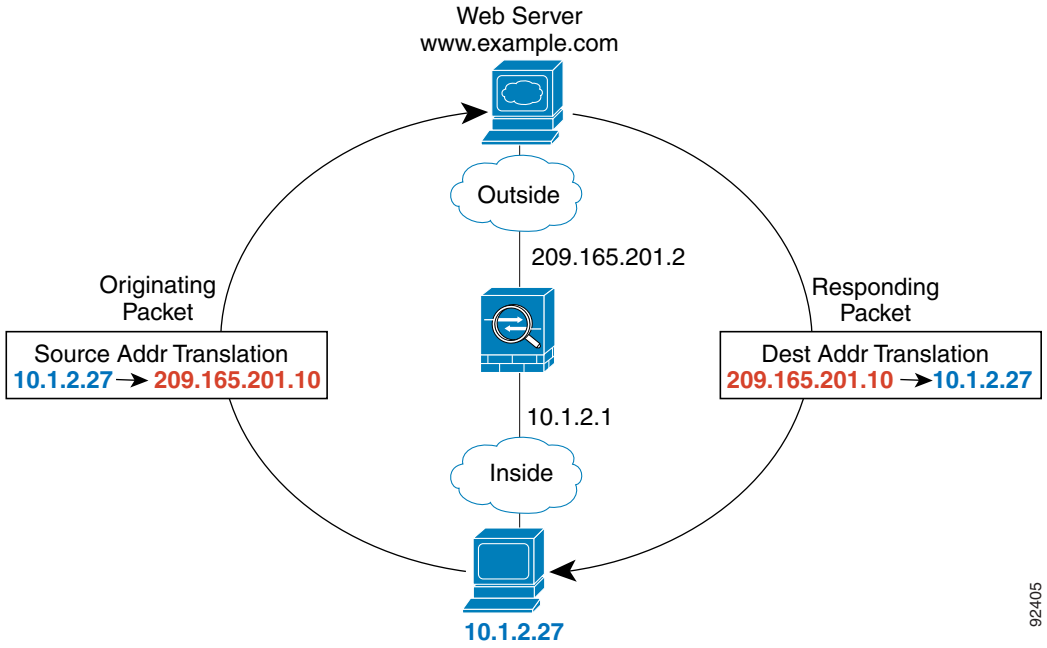
Note NAT control was the default behavior for software versions earlier than Version 7.0. If you upgrade a security appliance from an earlier version, then the **nat-control** command is automatically added to your configuration to maintain the expected behavior.

Some of the benefits of NAT include the following:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a host.
- NAT can resolve IP routing problems by supporting overlapping IP addresses.

Figure 12-1 shows a typical NAT scenario, with a private network on the inside. When the inside user sends a packet to a web server on the Internet, the local source address of the packet is changed to a routable global address. When the web server responds, it sends the response to the global address, and the security appliance receives the packet. The security appliance then translates the global address to the local address before sending it on to the user.

Figure 12-1 NAT Example



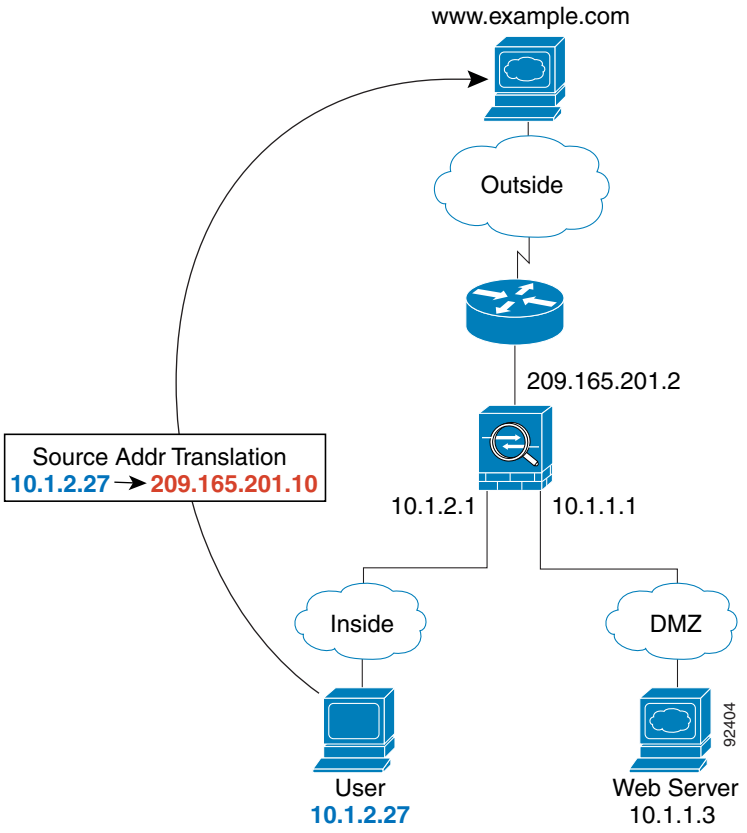
How Data Moves Through the Security Appliance in Routed Firewall Mode

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

Figure 12-2 shows an inside user accessing an outside web server.

Figure 12-2 Inside to Outside



The following steps describe how data moves through the security appliance (see Figure 12-2):

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.

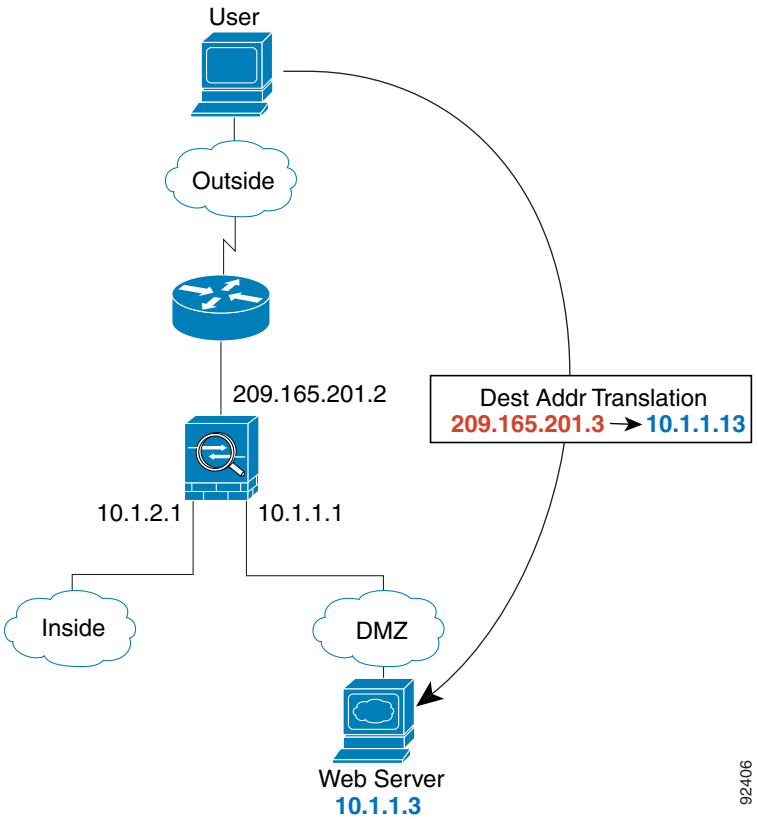
   The global address could be on any subnet, but routing is simplified when it is on the outside interface subnet.
4. The security appliance then records that a session is established and forwards the packet from the outside interface.

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 12-3 shows an outside user accessing the DMZ web server.

Figure 12-3 Outside to DMZ



The following steps describe how data moves through the security appliance (see Figure 12-3):

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).

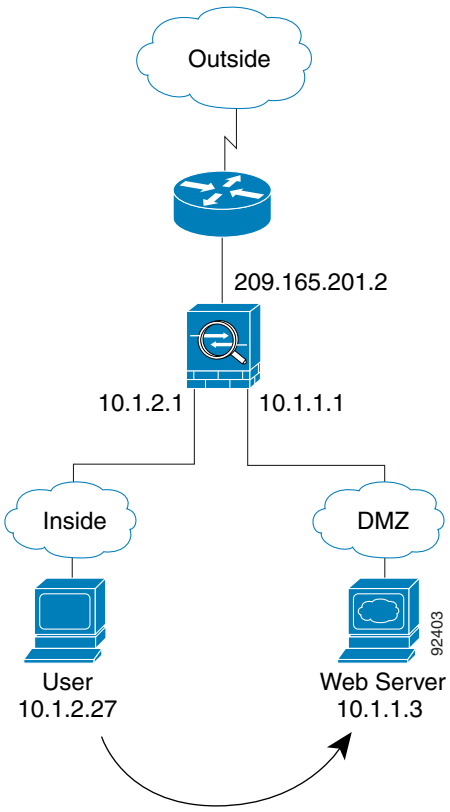
   For multiple context mode, the security appliance first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the classifier "knows" that 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 12-4 shows an inside user accessing the DMZ web server.

Figure 12-4 Inside to DMZ



The following steps describe how data moves through the security appliance (see Figure 12-4):

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).

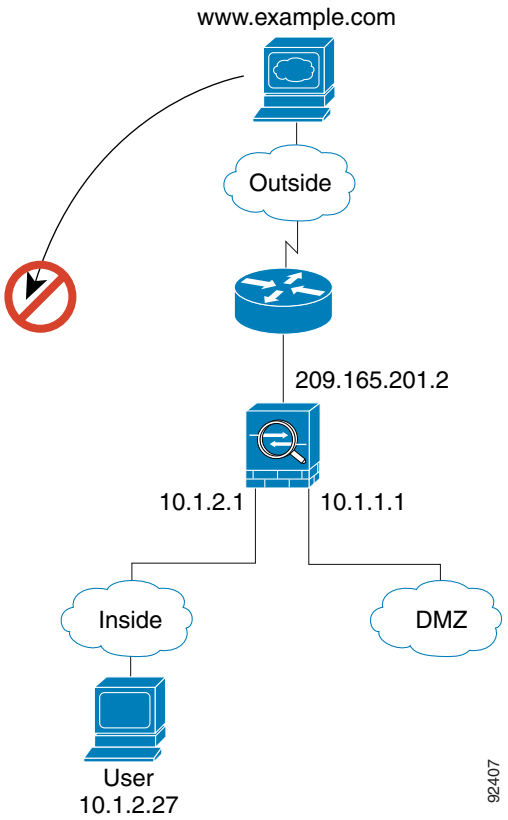
   For multiple context mode, the security appliance first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the interface is unique; 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 12-5 shows an outside user attempting to access the inside network.

Figure 12-5 Outside to Inside



The following steps describe how data moves through the security appliance (see Figure 12-5):

1. A user on the outside network attempts to reach an inside host (assuming the host has a routable IP address).

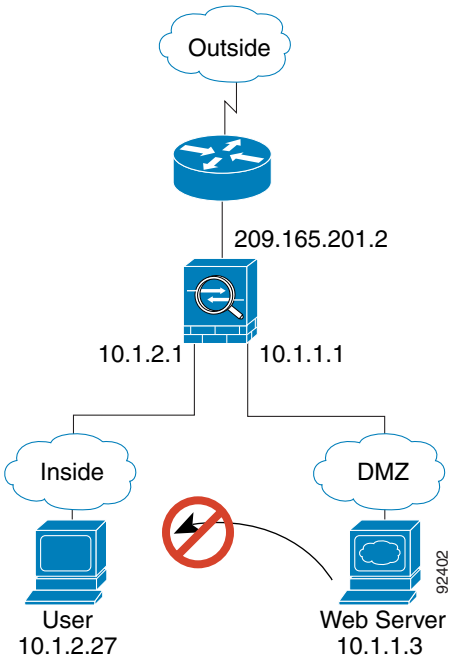
   If the inside network uses private addresses, no outside user can reach the inside network without NAT. The outside user might attempt to reach an inside user by using an existing NAT session.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies 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 12-6 shows a user in the DMZ attempting to access the inside network.

Figure 12-6 DMZ to Inside



The following steps describe how data moves through the security appliance (see Figure 12-6):

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).
3. The packet is denied, and the security appliance drops the packet and logs the connection attempt.

Transparent Mode Overview

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

Transparent Firewall Features

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

Maintenance is facilitated because there are no complicated routing patterns to troubleshoot and no NAT configuration.

Even though transparent mode acts as a bridge, Layer 3 traffic, such as IP traffic, cannot pass through the security appliance unless you explicitly permit it with an extended access list. The only traffic allowed through the transparent firewall without an access list is ARP traffic. ARP traffic can be controlled by ARP inspection.

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 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.

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.

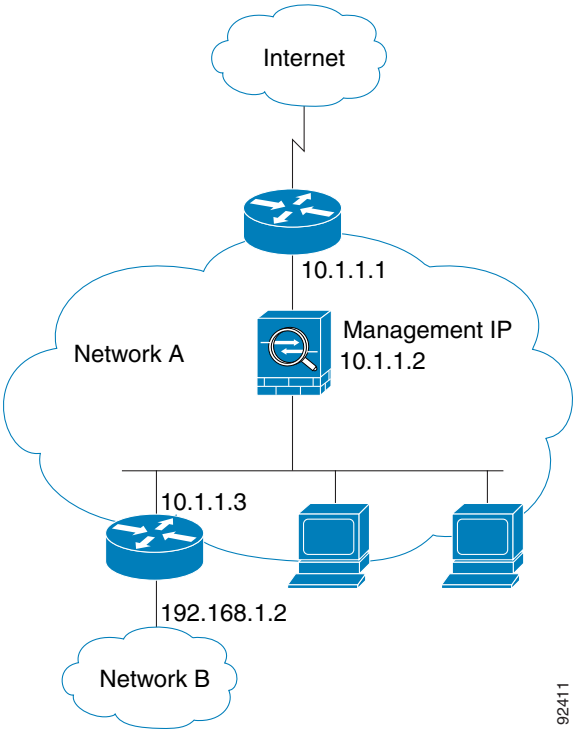
For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality. For example, by using an extended access list, you can allow DHCP traffic (instead of the unsupported DHCP relay feature)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

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 statements can still be configured, but they only apply to security appliance-originated traffic. 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.

Using the Transparent Firewall in Your Network

Figure 12-7 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 12-7 Transparent Firewall Network



Transparent Firewall Guidelines

Follow these guidelines when planning your transparent firewall network:

- A management IP address is required; 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).

- 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.

  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.
- You must use an extended access list to allow Layer 3 traffic, such as IP traffic, through the security appliance.

  You can also optionally use an EtherType access list to allow non-IP traffic through.

Unsupported Features in Transparent Mode

The following features are not supported in transparent mode:

- NAT

  NAT is performed on the upstream router.
- 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.
- IPv6
- 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 an extended access list.
- Quality of Service
- Multicast

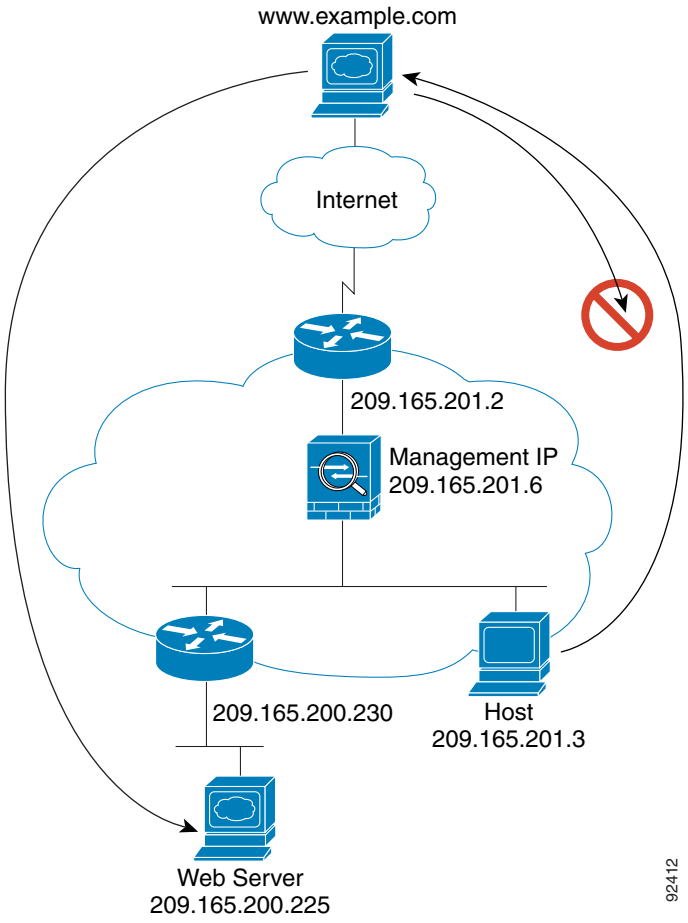
  You can, however, allow multicast traffic through the security appliance by allowing it in an extended access list.
- VPN termination for through traffic

  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.

How Data Moves Through the Transparent Firewall

Figure 12-8 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 12-8 Typical Transparent Firewall Data Path



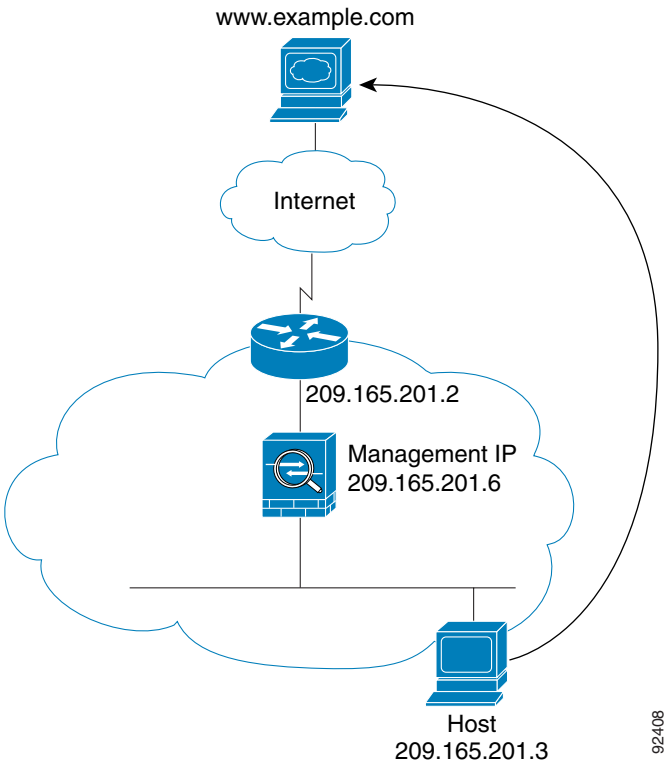
This section describes how data moves through the security appliance, and includes the following topics:

- An Inside User Visits a Web Server, page 12-13
- An Outside User Visits a Web Server on the Inside Network, page 12-14
- An Outside User Attempts to Access an Inside Host, page 12-15

An Inside User Visits a Web Server

Figure 12-9 shows an inside user accessing an outside web server.

Figure 12-9 Inside to Outside



The following steps describe how data moves through the security appliance (see Figure 12-9):

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).

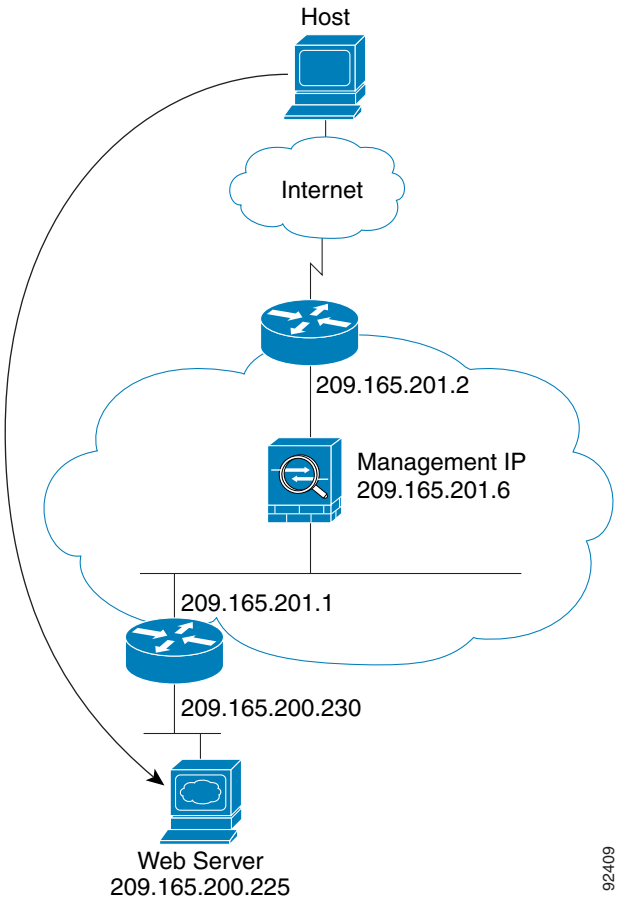
   For multiple context mode, the security appliance first classifies the packet according to a unique interface.
3. The security appliance and records that a session is established.
4. If the destination MAC address is in its table, the security appliance forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 209.186.201.2.

   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 or a ping. The first packet is dropped.
5. When the web server responds to the request, the security appliance adds the web server MAC address to the MAC address table, if required, and 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 Outside User Visits a Web Server on the Inside Network

Figure 12-10 shows an outside user accessing the inside web server.

Figure 12-10 Outside to Inside



The following steps describe how data moves through the security appliance (see Figure 12-10):

1. A user on the outside network requests a web page from the inside web server.
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 inside interface. The destination MAC address is that of the downstream router, 209.186.201.1.

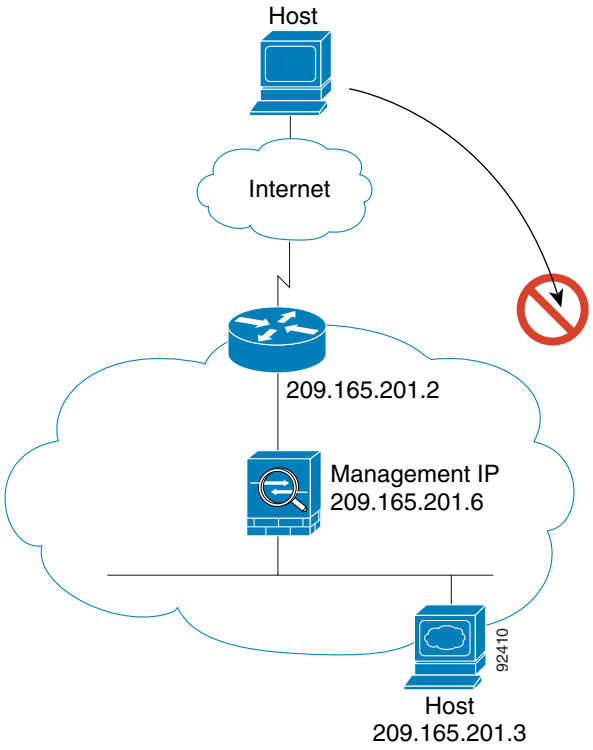
   If the destination MAC address is not in the security appliance table, the security appliance attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.
5. When the web server responds to the request, the security appliance adds the web server MAC address to the MAC address table, if required, and 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 12-11 shows an outside user attempting to access a host on the inside network.

Figure 12-11 Outside to Inside



The following steps describe how data moves through the security appliance (see Figure 12-11):

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, 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.