



# CHAPTER 15

## Firewall Mode Overview

---

This chapter describes how the firewall works in each firewall mode. To set the firewall mode, see the “[Setting Transparent or Routed Firewall Mode](#)” section on [page 2-5](#).



### 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:

- [Routed Mode Overview, page 15-1](#)  
[Transparent Mode Overview, page 15-8](#)

## Routed Mode Overview

NAT between connected networks, and 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.

This section includes the following topics:

- [IP Routing Support, page 15-1](#)
- [Network Address Translation, page 15-2](#)
- [How Data Moves Through the Security Appliance in Routed Firewall Mode, page 15-3](#)

## 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. 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

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**



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:

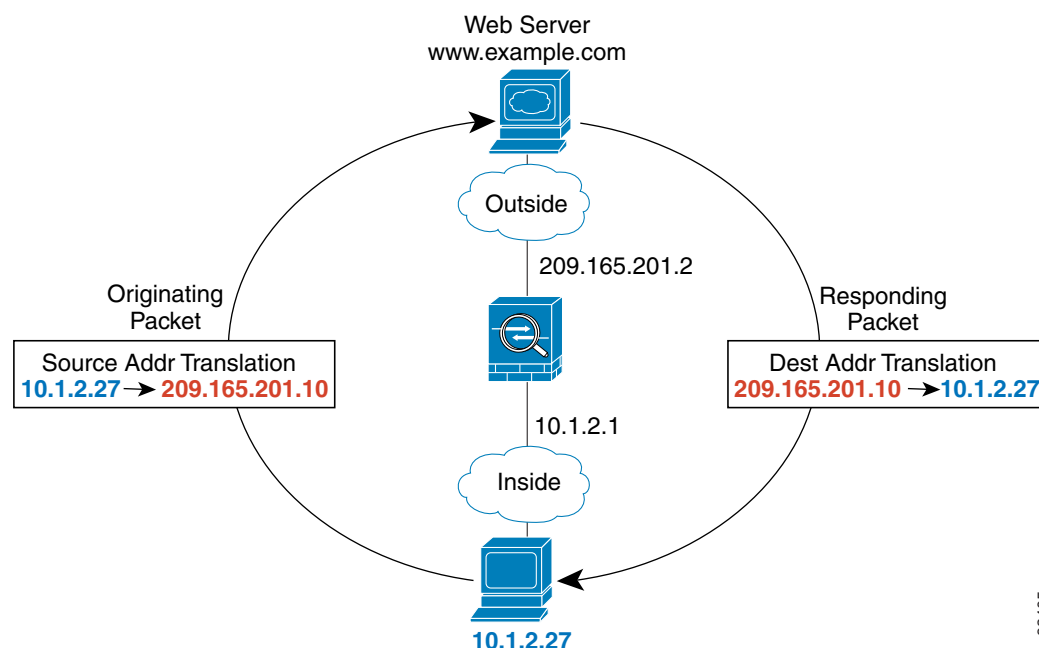
- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.

- 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 15-1 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 15-1** NAT Example



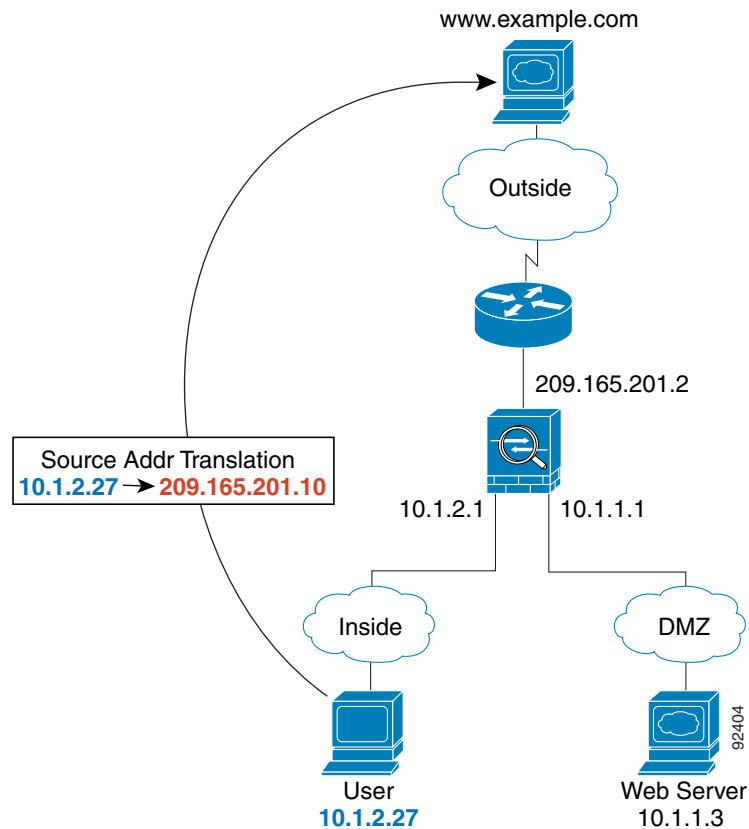
92405

## How Data Moves Through the Security Appliance in Routed Firewall Mode

- [An Inside User Visits a Web Server, page 15-3](#)
- [An Outside User Visits a Web Server on the DMZ, page 15-4](#)
- [An Inside User Visits a Web Server on the DMZ, page 15-6](#)
- [An Outside User Attempts to Access an Inside Host, page 15-7](#)
- [A DMZ User Attempts to Access an Inside Host, page 15-8](#)

### An Inside User Visits a Web Server

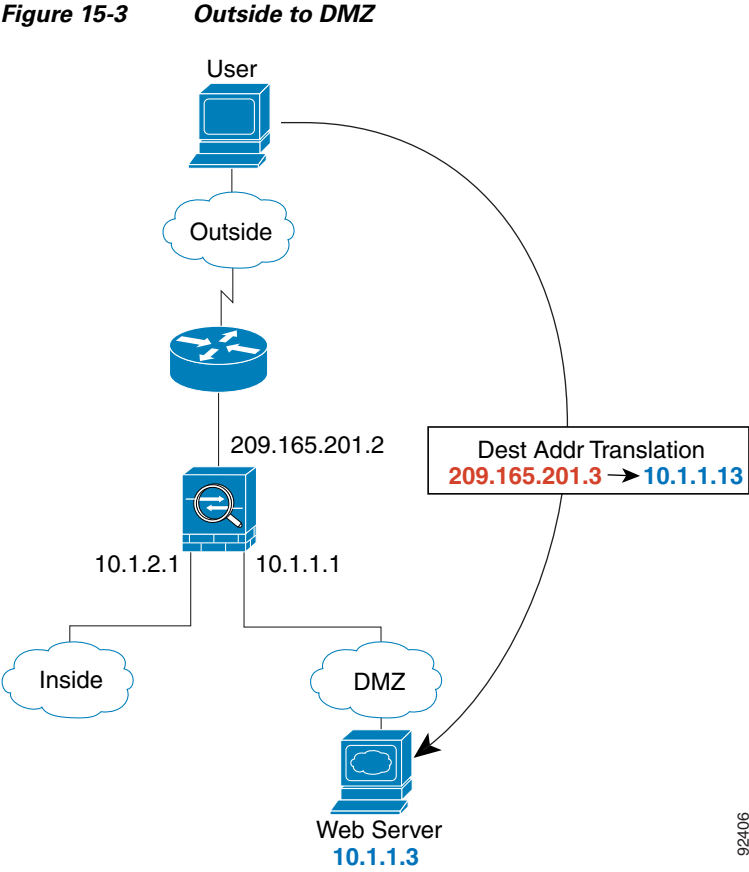
Figure 15-2 Inside to Outside

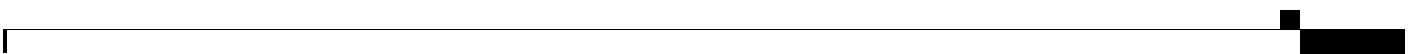
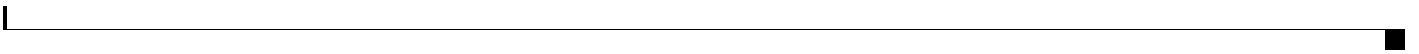


- 1.
- 2.

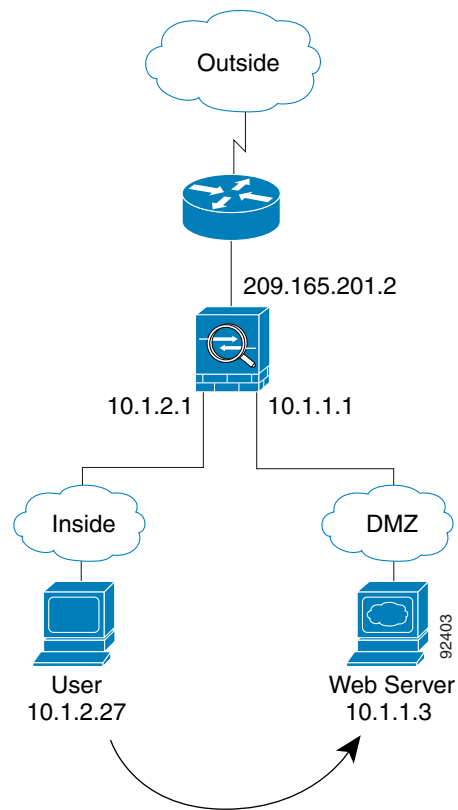
- 3. 209.165.201.10, which is on the outside interface subnet.  
The global address could be on any subnet, but routing is simplified when it is on the outside interface subnet.
- 4. The security appliance then records that a session is established and forwards the packet from the outside interface.
- 5.
- 6.

### An Outside User Visits a Web Server on the DMZ

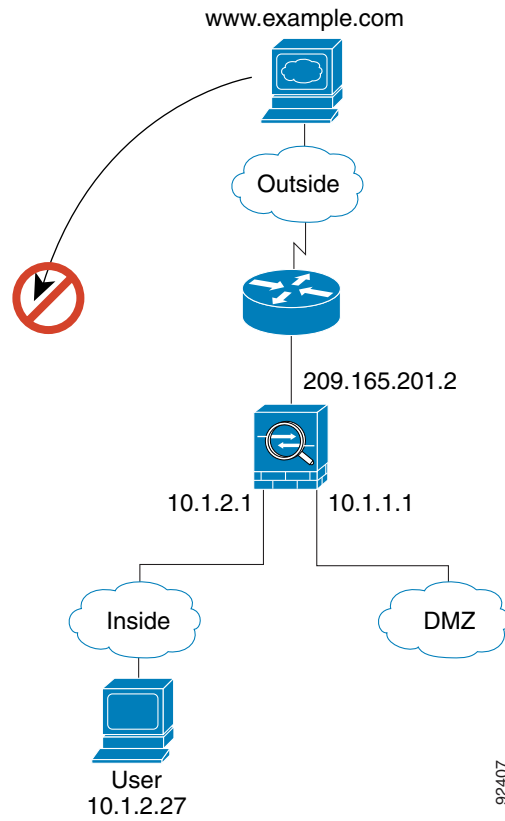




**Figure 15-4**    *Inside to DMZ*



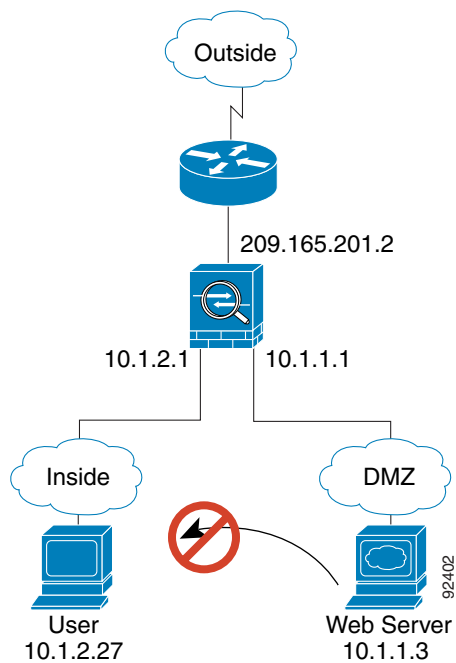
## An Outside User Attempts to Access an Inside Host



- 1.
- 2.
- 3.

## A DMZ User Attempts to Access an Inside Host

Figure 15-6 DMZ to Inside



## Transparent Mode Overview

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 15-9](#)
  - [Allowing Layer 3 Traffic, page 15-9](#)
  - [Passing Traffic Not Allowed in Routed Mode, page 15-9](#)
  - [MAC Address Lookups, page 15-10](#)
- [Using the Transparent Firewall in Your Network, page 15-10](#)
- [Transparent Firewall Guidelines, page 15-10](#)

[Unsupported Features in Transparent Mode, page 15-11](#)

[How Data Moves Through the Transparent Firewall, page 15-13](#)

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; IP readdressing is unnecessary.

## Allowing Layer 3 Traffic

## Allowed MAC Addresses

- 
- 
- 
- 
- 

## Passing Traffic Not Allowed in Routed Mode



---

### Note

---

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.

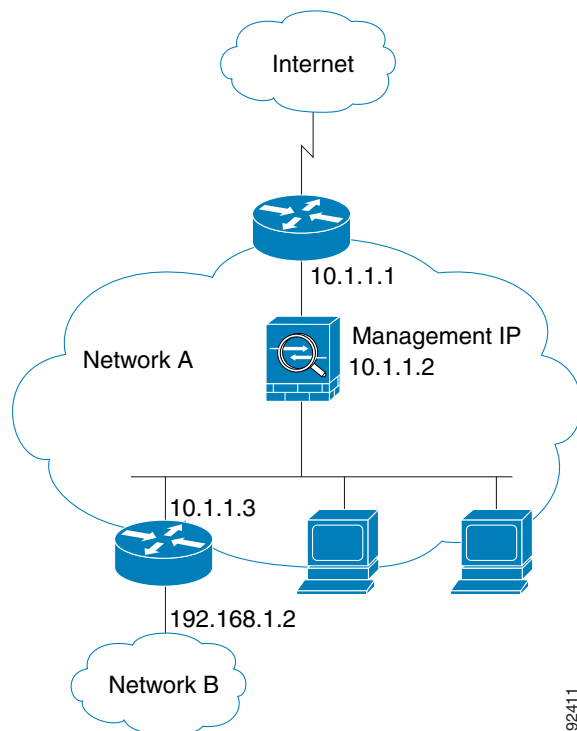
Non-IP traffic (for example AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through using an EtherType access list.

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 15-7** *Transparent Firewall Network*



92411

## Transparent Firewall Guidelines

- 




---

**Note**


---

- 

- 

- 

- 

- 

## Unsupported Features in Transparent Mode

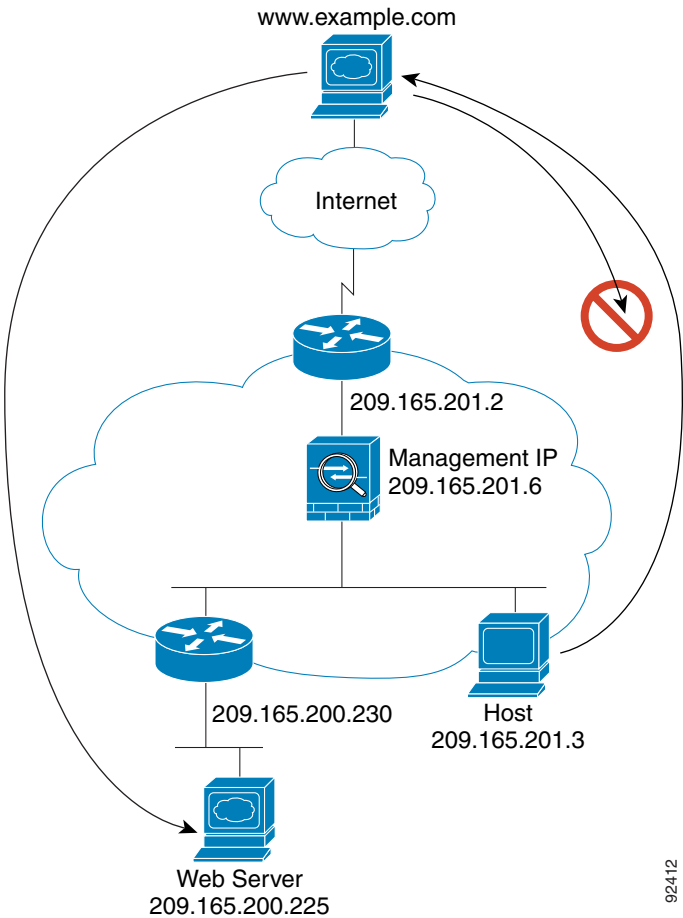
**Table 15-1** *Unsupported Features in Transparent Mode*

Feature	Description
—	—
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.

**Unsupported Features in Transparent Mode (continued)**

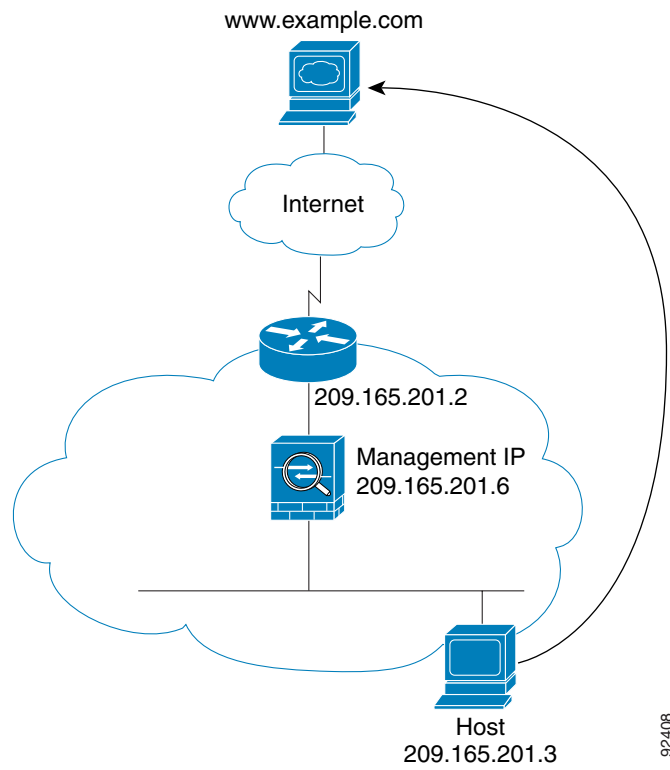
Dynamic routing protocols	You can, however, add static routes for traffic originating on the security appliance. You can also allow dynamic routing protocols through the security appliance using an extended access list.
IPv6	You also cannot allow IPv6 using an EtherType access list.
Multicast	You can allow multicast traffic through the security appliance by allowing it in an extended access list.
NAT	NAT is performed on the upstream router.
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. WebVPN is also not supported.

**Figure 15-8** Typical Transparent Firewall Data Path



92412

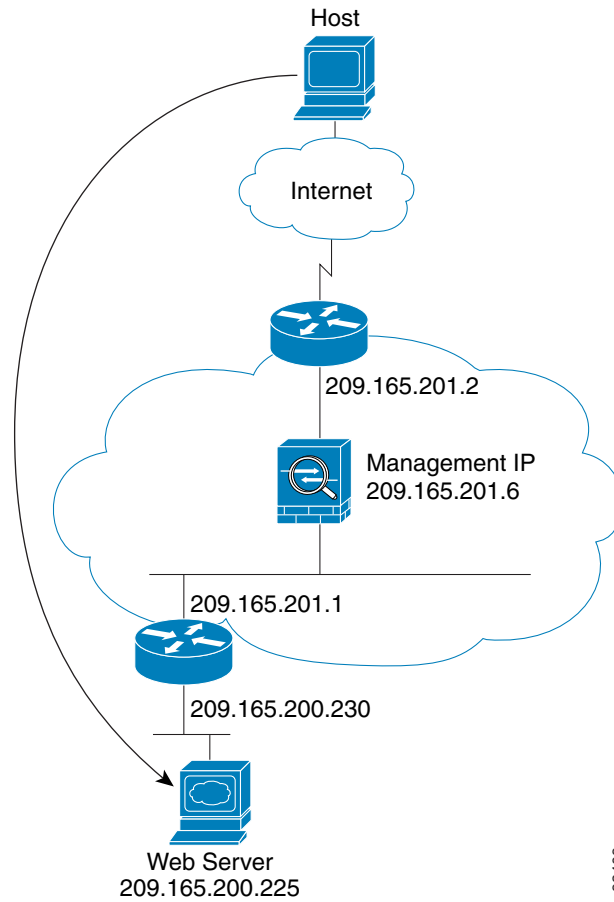
**Figure 15-9**     *Inside to Outside*



92408

## An Outside User Visits a Web Server on the Inside Network

Figure 15-10 Outside to Inside



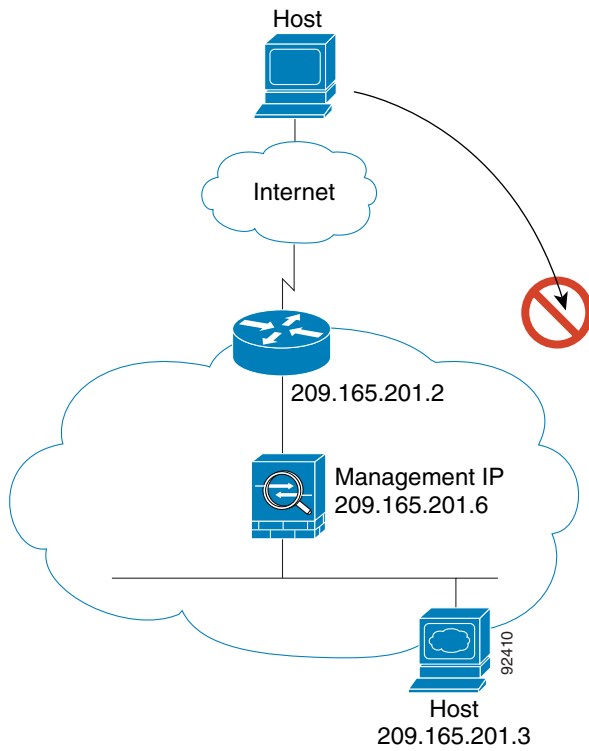
92409

- 1.
- 2.
- 3.
- 4.
- 5.

6.

### An Outside User Attempts to Access an Inside Host

Figure 15-11 Outside to Inside



1.

2.

3.

4.