CHAPTER 43

Troubleshooting the Security Appliance

This chapter describes how to troubleshoot the security appliance, and includes the following sections:

Testing Your Configuration

This section describes how to test connectivity for the single mode security appliance or for each security context. The following steps describe how to ping the security appliance interfaces, and how to allow hosts on one interface to ping hosts on another interface.

We recommend that you only enable pinging and debug messages during troubleshooting. When you are done testing the security appliance, follow the steps in the "Disabling the Test Configuration" section on page 43-5.

This section includes the following topics:

Enabling ICMP Debug Messages and System Messages

Debug messages and system messages can help you troubleshoot why your pings are not successful. The security appliance only shows ICMP debug messages for pings to the security appliance interfaces, and not for pings through the security appliance to other hosts. To enable debugging and system messages, perform the following steps:

Step 1 To show ICMP packet information for pings to the security appliance interfaces, enter the following command:

```
hostname(config)# debug icmp trace
```

Step 2 To set system messages to be sent to Telnet or SSH sessions, enter the following command:

```
hostname(config)# logging monitor debug
```

You can alternately use **logging buffer debug** to send messages to a buffer, and then view them later using the **show logging** command.

Step 3 To send the system messages to your Telnet or SSH session, enter the following command:

```
hostname(config)# terminal monitor
```

Step 4 To enable system messages, enter the following command:

```
hostname(config)# logging on
```

The following example shows a successful ping from an external host (209.165.201.2) to the security appliance outside interface (209.165.201.1):

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

The preceding example shows the ICMP packet length (32 bytes), the ICMP packet identifier (1), and the ICMP sequence number (the ICMP sequence number starts at 0 and is incremented each time a request is sent).

Pinging Security Appliance Interfaces

To test that the security appliance interfaces are up and running and that the security appliance and connected routers are routing correctly, you can ping the security appliance interfaces.

Note For security purposes the security appliance does not support far-end interface ping, that is pinging the IP address of the outside interface from the inside network.

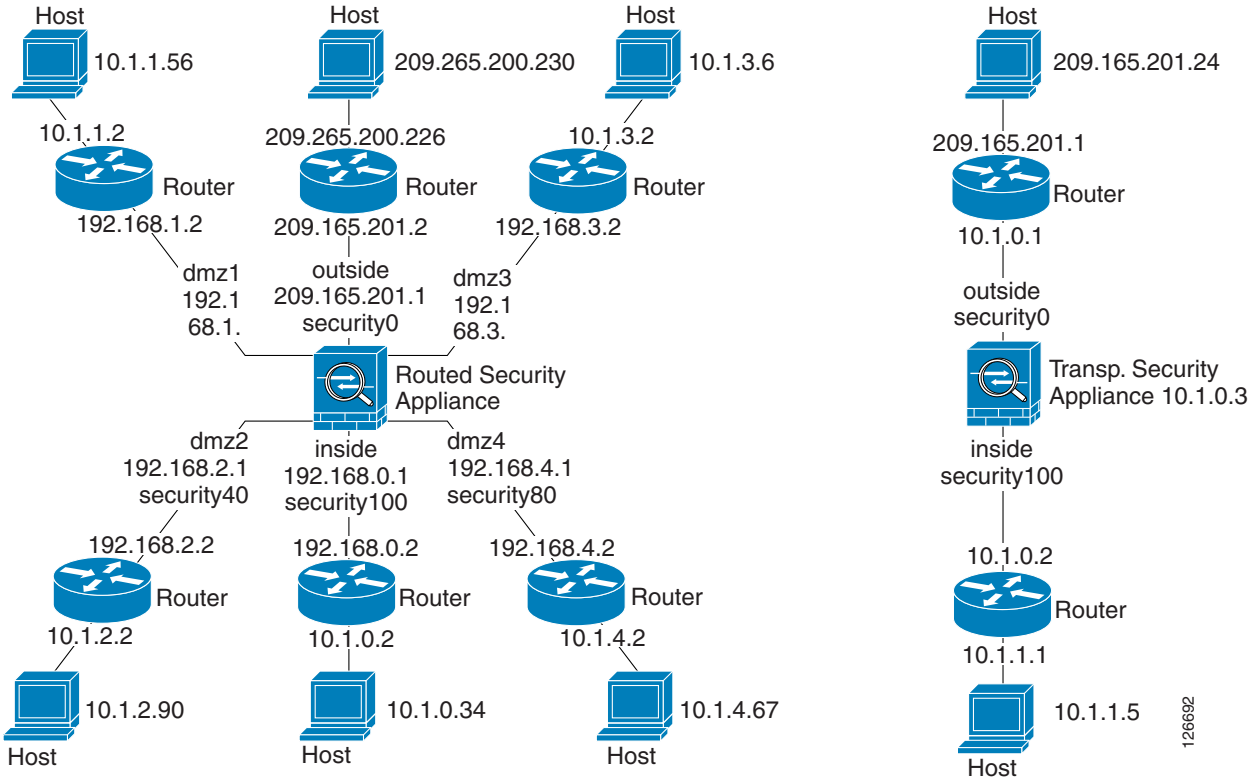
To ping the security appliance interfaces, perform the following steps:

Step 1 Create a sketch of your single mode security appliance or security context showing the interface names, security levels, and IP addresses.

Note Although this procedure uses IP addresses, the **ping** command also supports DNS names and names assigned to a local IP address with the **name** command.

The sketch should also include any directly connected routers, and a host on the other side of the router from which you will ping the security appliance. You will use this information for this procedure as well as the procedure in the "Pinging Through the Security Appliance" section on page 43-4. For example:

Figure 43-1 Network Sketch with Interfaces, Routers, and Hosts

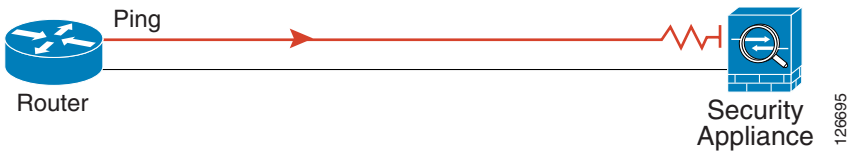


Step 2 Ping each security appliance interface from the *directly connected* routers. For transparent mode, ping the management IP address.

This test ensures that the security appliance interfaces are active and that the interface configuration is correct.

A ping might fail if the security appliance interface is not active, the interface configuration is incorrect, or if a switch between the security appliance and router is down (see Figure 43-2). In this case, no debug messages or system messages appear on the security appliance, because the packet never reaches it.

Figure 43-2 Ping Failure at Security Appliance Interface

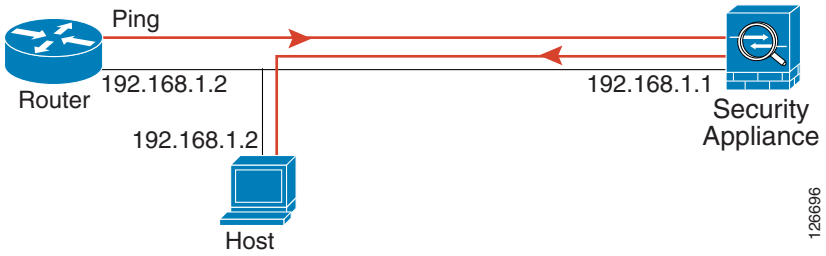


If the ping reaches the security appliance, and the security appliance responds, you see debug messages like the following:

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

If the ping reply does not return to the router, then you might have a switch loop or redundant IP addresses (see Figure 43-3).

Figure 43-3 Ping Failure Because of IP Addressing Problems

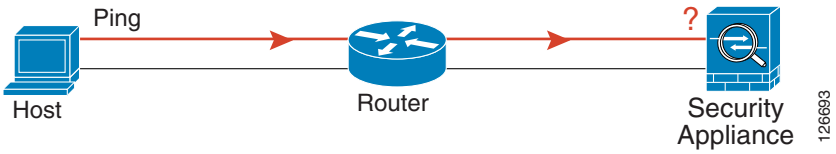


Step 3 Ping each security appliance interface from a remote host. For transparent mode, ping the management IP address.

This test checks that the directly connected router can route the packet between the host and the security appliance, and that the security appliance can correctly route the packet back to the host.

A ping might fail if the security appliance does not have a route back to the host through the intermediate router (see Figure 43-4). In this case, the debug messages show that the ping was successful, but you see system message 110001 indicating a routing failure.

Figure 43-4 Ping Failure Because the Security Appliance has no Route



Pinging Through the Security Appliance

After you successfully ping the security appliance interfaces, you should make sure traffic can pass successfully through the security appliance. For routed mode, this test shows that NAT is working correctly, if configured. For transparent mode, which does not use NAT, this test confirms that the security appliance is operating correctly; if the ping fails in transparent mode, contact Cisco TAC.

To ping between hosts on different interfaces, perform the following steps:

Step 1 To add an access list allowing ICMP from any source host, enter the following command:

```
hostname(config)# access-list ICMPACL extended permit icmp any any
```

By default, when hosts access a lower security interface, all traffic is allowed through. However, to access a higher security interface, you need the preceding access list.

Step 2 To assign the access list to each source interface, enter the following command:

```
hostname(config)# access-group ICMPACL in interface interface_name
```

Repeat this command for each source interface.

Step 3 To enable the ICMP inspection engine, so ICMP responses are allowed back to the source host, enter the following commands:

```
hostname(config)# class-map ICMP-CLASS
```

```
hostname(config-cmap)# match access-list ICMPACL
hostname(config-cmap)# policy-map ICMP-POLICY
hostname(config-pmap)# class ICMP-CLASS
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# service-policy ICMP-POLICY global
```

Alternatively, you can also apply the ICMPACL access list to the destination interface to allow ICMP traffic back through the security appliance.

Step 4 Ping from the host or router through the source interface to another host or router on another interface.

Repeat this step for as many interface pairs as you want to check.

If the ping succeeds, you see a system message confirming the address translation for routed mode (305009 or 305011) and that an ICMP connection was established (302020). You can also enter the **show xlate** and **show conns** commands to view this information.

If the ping fails for transparent mode, contact Cisco TAC.

For routed mode, the ping might fail because NAT is not configured correctly (see Figure 43-5). This is more likely if you enable NAT control. In this case, you see a system message showing that the NAT translation failed (305005 or 305006). If the ping is from an outside host to an inside host, and you do not have a static translation (which is required with NAT control), you see message 106010: deny inbound icmp.

Note The security appliance only shows ICMP debug messages for pings to the security appliance interfaces, and not for pings through the security appliance to other hosts.

Figure 43-5 Ping Failure Because the Security Appliance is not Translating Addresses

Disabling the Test Configuration

After you complete your testing, disable the test configuration that allows ICMP to and through the security appliance and that prints debug messages. If you leave this configuration in place, it can pose a serious security risk. Debug messages also slow the security appliance performance.

To disable the test configuration, perform the following steps:

Step 1 To disable ICMP debug messages, enter the following command:

```
hostname(config)# no debug icmp trace
```

Step 2 To disable logging, if desired, enter the following command:

```
hostname(config)# no logging on
```

Step 3 To remove the ICMPACL access list, and also delete the related **access-group** commands, enter the following command:

```
hostname(config)# no access-list ICMPACL
```

Step 4 (Optional) To disable the ICMP inspection engine, enter the following command:

```
hostname(config)# no service-policy ICMP-POLICY
```

Traceroute

You can trace the route of a packet using the traceroute feature, which is accessed with the **traceroute** command. A traceroute works by sending UDP packets to a destination on an invalid port. Because the port is not valid, the routers along the way to the destination will respond with an ICMP Time Exceeded Message, and report that error back to the security appliance.

Packet Tracer

In addition to capturing packets and the traceroute feature, it is possible to trace the lifespan of a packet through the security appliance to see if it is behaving as expected with the packet tracer tool. The packet tracer tool lets you do the following:

- Debug all packet drops in production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet along with the CLI lines which caused the rule addition.
- Show a time line of packet changes in a data path.
- Inject tracer packets into the data path.

The **packet-tracer** command provides detailed information about the packets and how they are processed by the security appliance. In the instance that a command from the configuration did not cause the packet to drop, the **packet-tracer** command will provide information about the cause in an easily readable manner. For example if a packet was dropped because of an invalid header validation, a message is displayed that says, “packet dropped due to bad ip header (reason).”

Note The **packet-tracer** command can generate packets based on the 5 tuple information—source IP, destination IP, source port, destination port, and protocol. The packet tracer does not populate the data part of the packet and as a result some engine checks will not be applicable. The packet tracer will show that the packet is dropped not because it did not pass the inspection checks but because there is not enough data to test against the inspection checks. For example the packet tracer will show drops incorrectly for dns traffic if the dns inspection is enabled.

Reloading the Security Appliance

In multiple mode, you can only reload from the system execution space. To reload the security appliance, enter the following command:

```
hostname# reload
```

Performing Password Recovery

This section describes how to recover if you forget passwords, or you create a lockout situation because of AAA settings. You can also disable password recovery for extra security. This section includes the following topics:

Performing Password Recovery for the ASA 5500 Series Adaptive Security Appliance

To recover passwords, perform the following steps:

Step 1 Connect to the security appliance console port according to the "Accessing the Command-Line Interface" section on page 2-4.

Step 2 Power off the security appliance, and then power it on.

Step 3 During the startup messages, press the **Escape** key when prompted to enter ROMMON.

Step 4 To set the security appliance to ignore the startup configuration at reload, enter the following command:

```
rommon #1> confreg
```

The security appliance displays the current configuration register value, and asks if you want to change the value:

```
Current Configuration Register: 0x00000011
Configuration Summary:
  boot TFTP image, boot default image from Flash on netboot failure
Do you wish to change this configuration? y/n [n]:
```

Step 5 Record your current configuration register value, so you can restore it later.

Step 6 At the prompt, enter **Y** to change the value.

The security appliance prompts you for new values.

Step 7 Accept the default values for all settings, except for the "disable system configuration?" value; at that prompt, enter **Y**.

Step 8 Reload the security appliance by entering the following command:

```
rommon #2> boot
```

The security appliance loads a default configuration instead of the startup configuration.

Step 9 Enter privileged EXEC mode by entering the following command:

```
hostname> enable
```

Step 10 When prompted for the password, press **Return**.

The password is blank.

Step 11 Load the startup configuration by entering the following command:

```
hostname# copy startup-config running-config
```

Step 12 Enter global configuration mode by entering the following command:

```
hostname# configure terminal
```

Step 13 Change the passwords in the configuration by entering the following commands, as necessary:

```
hostname(config)# password password
hostname(config)# enable password password
hostname(config)# username name password password
```

Step 14 Change the configuration register to load the startup configuration at the next reload by entering the following command:

```
hostname(config)# config-register value
```

Where *value* is the configuration register value you noted in Step 5 and 0x1 is the default configuration register. For more information about the configuration register, see the *Cisco Security Appliance Command Reference*.

Step 15 Save the new passwords to the startup configuration by entering the following command:

```
hostname(config)# copy running-config startup-config
```

Password Recovery for the PIX 500 Series Security Appliance

Performing password recovery on the security appliance erases the login password, enable password, and **aaa authentication console** commands. To erase these commands so you can log in with the default passwords, perform the following steps:

Step 1 Download the PIX password tool from Cisco.com to a TFTP server accessible from the security appliance. See the link in the "Password Recovery Procedure for the PIX" document at the following URL:

```
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_password_recovery09186a008009478b.shtml
```

Step 2 Connect to the security appliance console port according to the "Accessing the Command-Line Interface" section on page 2-4.

Step 3 Power off the security appliance, and then power it on.

Step 4 Immediately after the startup messages appear, press the **Escape** key to enter monitor mode.

Step 5 Configure the network settings for the interface that accesses the TFTP server by entering the following commands:

```
monitor> interface interface_id
monitor> address interface_ip
monitor> server tftp_ip
monitor> file pw_tool_name
monitor> gateway gateway_ip
```

Step 6 Download the PIX password tool from the TFTP server by entering the following command:

```
monitor> tftp
```

If you have trouble reaching the server, you can enter the **ping** *address* command to test the connection.

Step 7 At the "Do you wish to erase the passwords?" prompt, enter **Y**.

You can now log in with the default login password of "cisco" and the blank enable password.

The following example shows the PIX password recovery with the TFTP server on the outside interface:

```
monitor> interface 0
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7 )

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10), MAC: 0050.54ff.82b9
monitor> address 10.21.1.99
address 10.21.1.99
monitor> server 172.18.125.3
server 172.18.125.3
monitor> file np70.bin
file np52.bin
monitor> gateway 10.21.1.1
gateway 10.21.1.1
monitor> ping 172.18.125.3
Sending 5, 100-byte 0xf8d3 ICMP Echoes to 172.18.125.3, timeout is 4 seconds:
!!!!!
Success rate is 100 percent (5/5)
monitor> tftp
tftp np52.bin@172.18.125.3 via 10.21.1.1.................................
Received 73728 bytes

Cisco PIX password tool (4.0) #0: Tue Aug 22 23:22:19 PDT 2005
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xd8000

Do you wish to erase the passwords? [yn] y
Passwords have been erased.

Rebooting....
```

Disabling Password Recovery

You might want to disable password recovery to ensure that unauthorized users cannot use the password recovery mechanism to compromise the security appliance. To disable password recovery, enter the following command:

```
hostname(config)# no service password-recovery
```

On the ASA 5500 series adaptive security appliance, the **no service password-recovery** command prevents a user from entering ROMMON with the configuration intact. When a user enters ROMMON, the security appliance prompts the user to erase all Flash file systems. The user cannot enter ROMMON without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on using ROMMON and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available. The **service password-recovery** command appears in the configuration file for informational purposes only; when you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable

password recovery when the security appliance is configured to ignore the startup configuration at startup (in preparation for password recovery), then the security appliance changes the setting to boot the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

On the PIX 500 series security appliance, the **no service password-recovery** command forces the PIX password tool to prompt the user to erase all Flash file systems. The user cannot use the PIX password tool without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available.

Resetting the Password on the SSM Hardware Module

To reset the password to the default of "cisco" on the SSM hardware module, perform the following steps:

Step 1 Make sure the SSM hardware module is in the Up state and supports password reset.

Step 2 Enter the following command:

```
hostname (config)# hw-module module 1 password-reset
```

Where *1* is the specified slot number on the SSM hardware module.

Note On the AIP SSM, entering this command reboots the hardware module. The module is offline until the rebooting is finished. Enter the **show module** command to monitor the module status. The AIP SSM supports this command in version 6.0 and later.

On the CSC SSM, entering this command resets web services on the hardware module after the password has been reset. You may lose connection to ASDM or be logged out of the hardware module. The CSC SSM supports this command in the most recent version of 6.1, dated November 2006.

```
Reset the password on module in slot 1? [confirm]
```

Step 3 Enter **y** to confirm.

Other Troubleshooting Tools

The security appliance provides other troubleshooting tools to be used in conjunction with Cisco TAC:

- Viewing Debug Messages, page 43-11
- Capturing Packets, page 43-11
- Viewing the Crash Dump, page 43-11

Viewing Debug Messages

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use. To enable debug messages, see the **debug** commands in the *Cisco Security Appliance Command Reference*.

Capturing Packets

Capturing packets is sometimes useful when troubleshooting connectivity problems or monitoring suspicious activity. We recommend contacting Cisco TAC if you want to use the packet capture feature. See the **capture** command in the *Cisco Security Appliance Command Reference*.

Viewing the Crash Dump

If the security appliance crashes, you can view the crash dump information. We recommend contacting Cisco TAC if you want to interpret the crash dump. See the **show crashdump** command in the *Cisco Security Appliance Command Reference*.

Common Problems

This section describes common problems with the security appliance, and how you might resolve them.

Symptom The context configuration was not saved, and was lost when you reloaded.

Possible Cause You did not save each context within the context execution space. If you are configuring contexts at the command line, you did not save the context before you changed to the next context.

Recommended Action Save each context within the context execution space using the **copy run start** command. You cannot save contexts from the system execution space.

Symptom You cannot make a Telnet connection or SSH to the security appliance interface.

Possible Cause You did not enable Telnet or SSH to the security appliance.

Recommended Action Enable Telnet or SSH to the security appliance according to the "Allowing Telnet Access" section on page 40-1 or the "Allowing SSH Access" section on page 40-2.

Symptom You cannot ping the security appliance interface.

Possible Cause You disabled ICMP to the security appliance.

Recommended Action Enable ICMP to the security appliance for your IP address using the **icmp** command.

Symptom You cannot ping through the security appliance, even though the access list allows it.

Possible Cause You did not enable the ICMP inspection engine or apply access lists on both the ingress and egress interfaces.

Recommended Action Because ICMP is a connectionless protocol, the security appliance does not automatically allow returning traffic through. In addition to an access list on the ingress interface, you either need to apply an access list to egress interface to allow replying traffic, or enable the ICMP inspection engine, which treats ICMP connections as stateful connections.

Symptom Traffic does not pass between two interfaces on the same security level.

Possible Cause You did not enable the feature that allows traffic to pass between interfaces on the same security level.

Recommended Action Enable this feature according to the "Allowing Communication Between Interfaces on the Same Security Level" section on page 7-6.