



CHAPTER 40

Troubleshooting the Security Appliance

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

- [Testing Your Configuration, page 40-1](#)
- [Reloading the Security Appliance, page 40-6](#)
- [Performing Password Recovery, page 40-6](#)
- [Using the ROM Monitor to Load a Software Image, page 40-10](#)
- [Erasing the Flash File System, page 40-11](#)
- [Other Troubleshooting Tools, page 40-11](#)
- [Common Problems, page 40-12](#)

Testing Your Configuration

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

We recommend that you only enable pinging and debug messages during troubleshooting. When you are done testing the adaptive security appliance, follow the steps in [“Disabling the Test Configuration” section on page 40-5](#).

This section includes the following topics:

- [Enabling ICMP Debug Messages and System Log Messages, page 40-1](#)
- [Pinging Security Appliance Interfaces, page 40-2](#)
- [Pinging Through the Security Appliance, page 40-4](#)
- [Disabling the Test Configuration, page 40-5](#)

Enabling ICMP Debug Messages and System Log Messages

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

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

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

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

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

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

- Step 3** To send the system log messages to a Telnet or SSH session, enter the following command:

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

- Step 4** To enable system log 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 adaptive 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
```

This 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 that a request is sent).

Pinging Security Appliance Interfaces

To test whether the adaptive security appliance interfaces are up and running and that the adaptive security appliance and connected routers are operating correctly, you can ping the adaptive security appliance interfaces. To ping the adaptive security appliance interfaces, perform the following steps:

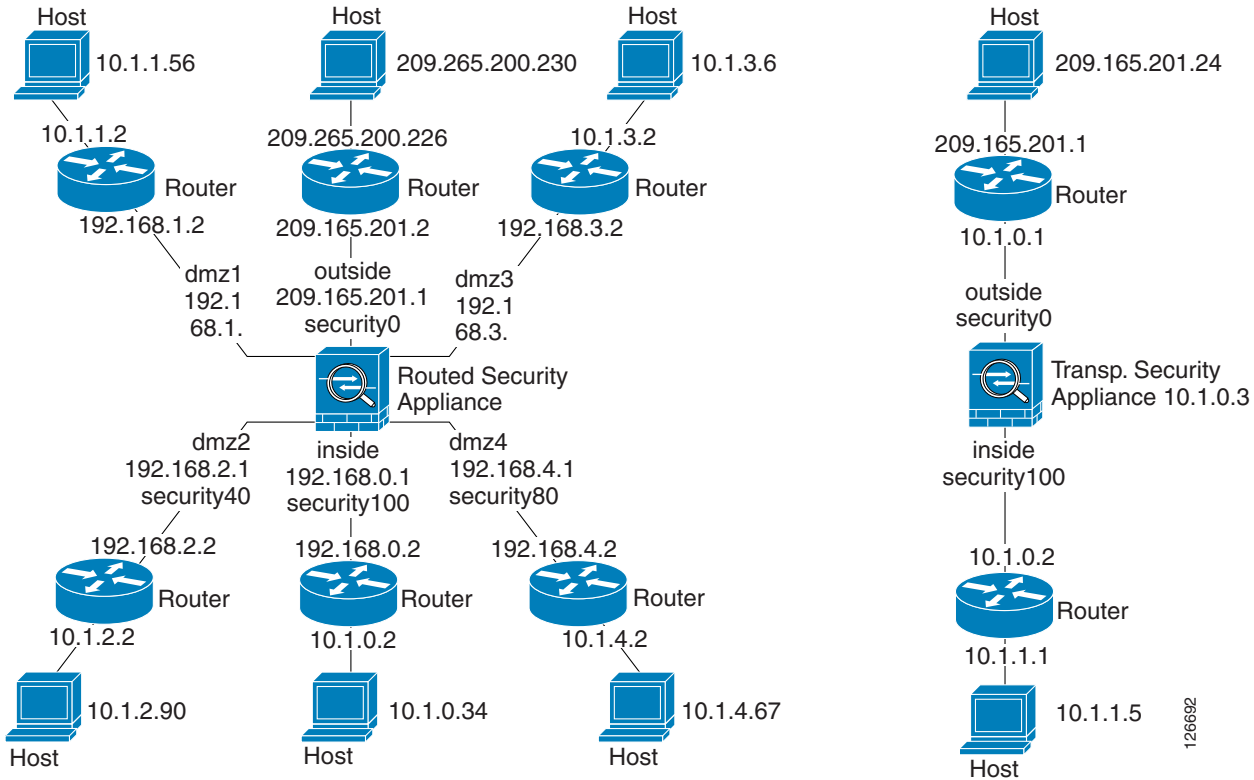
-
- Step 1** Draw a diagram of your single-mode adaptive security appliance or security context that shows the interface names, security levels, and IP addresses.



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

The diagram should also include any directly connected routers, and a host on the other side of the router from which you will ping the adaptive security appliance. You will use this information in this procedure and in the procedure in [“Pinging Through the Security Appliance”](#) section on page 40-4. For example:

Figure 40-1 Network Diagram with Interfaces, Routers, and Hosts



Step 2 Ping each adaptive security appliance interface from the directly connected routers. For transparent mode, ping the management IP address. This test ensures that the adaptive security appliance interfaces are active and that the interface configuration is correct.

A ping might fail if the adaptive security appliance interface is not active, the interface configuration is incorrect, or if a switch between the adaptive security appliance and a router is down (see Figure 40-2). In this case, no debug messages or system log messages appear, because the packet never reaches the adaptive security appliance.

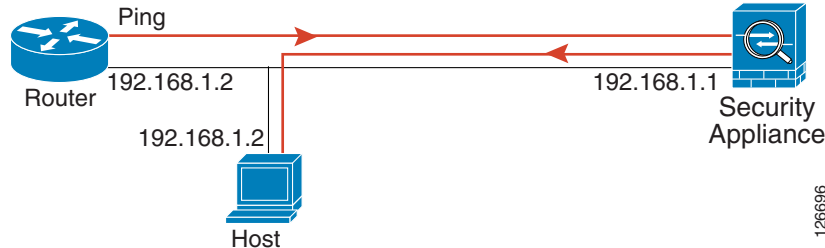
Figure 40-2 Ping Failure at Security Appliance Interface



If the ping reaches the adaptive security appliance, and the adaptive security appliance responds, debug messages similar to the following appear:

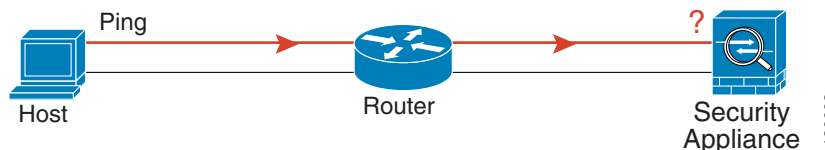
```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

If the ping reply does not return to the router, then a switch loop or redundant IP addresses may exist (see Figure 40-3).

Figure 40-3 Ping Failure Because of IP Addressing Problems

- Step 3** Ping each adaptive security appliance interface from a remote host. For transparent mode, ping the management IP address. This test checks whether the directly connected router can route the packet between the host and the adaptive security appliance, and whether the adaptive security appliance can correctly route the packet back to the host.

A ping might fail if the adaptive security appliance does not have a return route to the host through the intermediate router (see Figure 40-4). In this case, the debug messages show that the ping was successful, but system log message 110001 appears, indicating a routing failure.

Figure 40-4 Ping Failure Because the Security Appliance has no Return Route

Pinging Through the Security Appliance

After you successfully ping the adaptive security appliance interfaces, make sure traffic can pass successfully through the adaptive security appliance. For routed mode, this test shows that NAT is operating correctly, if configured. For transparent mode, which does not use NAT, this test confirms that the adaptive 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 and ensure that ICMP responses may return 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 ICMP access list to the destination interface to allow ICMP traffic back through the adaptive 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, a system log message appears to confirm the address translation for routed mode (305009 or 305011) and that an ICMP connection was established (302020). You can also enter either the **show xlate** or **show conns** command 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 40-5](#)). This failure is more likely to occur if you enable NAT control. In this case, a system log message appears, showing that the NAT failed (305005 or 305006). If the ping is from an outside host to an inside host, and you do not have a static translation (required with NAT control), the following system log message appears: “106010: deny inbound icmp.”



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

Figure 40-5 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 adaptive 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 adaptive 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 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 respond with an ICMP Time Exceeded Message, and report that error to the security appliance.

Packet Tracer

In addition, you can trace the lifespan of a packet through the security appliance to see whether the packet is operating correctly with the packet tracer tool. This tool lets you do the following:

- Debug all packet drops in a production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet, along with the CLI commands that 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. If 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, when a packet is dropped because of an invalid header validation, the following message appears: “packet dropped due to bad ip header (reason).”

Reloading the Security Appliance

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

```
hostname# reload
```

Performing Password Recovery

This section describes how to recover passwords if you have forgotten them or you are locked out because of AAA settings, and how to disable password recovery for extra security. This section includes the following topics:

- [Recovering Passwords for the ASA 5500 Series Adaptive Security Appliance](#), page 40-7
- [Recovering Passwords for the PIX 500 Series Security Appliance](#), page 40-8
- [Disabling Password Recovery](#), page 40-9

Recovering Passwords for the ASA 5500 Series Adaptive Security Appliance

To recover passwords for the ASA 5500 Series adaptive security appliance, perform the following steps:

- Step 1** Connect to the adaptive security appliance console port according to the instructions in “[Accessing the Command-Line Interface](#)” section on page 2-2
- Step 2** Power off the adaptive security appliance, and then power it on.
- Step 3** After startup, press the **Escape** key when you are prompted to enter ROMMON mode..
- Step 4** Issue the **confreg** command to view the current Configuration Register setting, and write it down so you can restore it later:

```
rommon #1> confreg
```

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

```
Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash
  ignore system configuration
Do you wish to change this configuration? y/n [n]: n

Select 'n'.
```

- Step 5** Set the configuration register to ignore the startup-config using a value of 0x41:

```
rommon #2> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

- Step 6** Reload the adaptive security appliance by entering the following command:

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.
Loading disk0:/asa822-k8.bin... Booting...Loading...
```

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

- Step 7** Access the privileged EXEC mode by entering the following command:

```
hostname(config)# enable
```

- Step 8** When prompted for the password, press **Enter**.

The password is blank.

- Step 9** Once in enable mode, copy the startup-config into the running config.

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

- Step 10** With your original config now loaded, set the new passwords.

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

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

- Step 11** Restore the original config-register that you saved earlier (Note: the default is 0x1).

```
hostname(config)# config-register 0x1
```

- Step 12** Finally, save the configuration with the new passwords.

```
hostname(config)# write memory
```

Recovering Passwords for the PIX 500 Series Security Appliance

Recovering passwords on the PIX 500 Series adaptive security appliance erases the login password, enable password, and **aaa authentication console** commands. To recover passwords for the PIX 500 Series adaptive security appliance, perform the following steps:

- Step 1** Download the PIX password tool from Cisco.com to a TFTP server accessible from the adaptive security appliance. For instructions, go to the following URL:

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

- Step 2** Connect to the adaptive security appliance console port according to the instructions in “[Accessing the Command-Line Interface](#)” section on page 2-2.

- Step 3** Power off the adaptive 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** In monitor mode, configure the interface network settings to access 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, 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 log in with the default login password of “cisco” and the blank enable password.

The following example shows password recovery on a PIX 500 Series adaptive security appliance 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 adaptive 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 mode with the configuration intact. When a user enters ROMMON mode, the adaptive security appliance prompts the user to erase all Flash file systems. The user cannot enter ROMMON mode without first performing this erasure. If a user chooses not to erase the Flash file system, the adaptive security appliance reloads. Because password recovery depends on using ROMMON mode 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 restore 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 information 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 adaptive security appliance is configured to ignore the startup configuration at startup (in preparation for password recovery), then the adaptive security appliance changes the setting to load 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 adaptive 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 restore the system to an operating state, load a new image and a backup configuration file, if available.

Using the ROM Monitor to Load a Software Image

This section describes how to load a software image to an adaptive security appliance from the ROM monitor mode using TFTP.

To load a software image to an adaptive security appliance, perform the following steps:

-
- Step 1** Connect to the adaptive security appliance console port according to the instructions in [“Accessing the Command-Line Interface”](#) section on page 2-2.
 - Step 2** Power off the adaptive security appliance, and then power it on.
 - Step 3** During startup, press the **Escape** key when you are prompted to enter ROMMON mode.
 - Step 4** In ROMMON mode, define the interface settings to the adaptive security appliance, including the IP address, TFTP server address, gateway address, software image file, and port, as follows:

```
rommon #1> ADDRESS=10.132.44.177
rommon #2> SERVER=10.129.0.30
rommon #3> GATEWAY=10.132.44.1
rommon #4> IMAGE=f1/asa800-232-k8.bin
rommon #5> PORT=Ethernet0/0
Ethernet0/0
Link is UP
MAC Address: 0012.d949.15b8
```



Note Be sure that the connection to the network already exists.

- Step 5** To validate your settings, enter the **set** command.

```
rommon #6> set
ROMMON Variable Settings:
ADDRESS=10.132.44.177
SERVER=10.129.0.30
GATEWAY=10.132.44.1
PORT=Ethernet0/0
VLAN=untagged
IMAGE=f1/asa800-232-k8.bin
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20
```

- Step 6** Ping the TFTP server by entering the **ping server** command.

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.129.0.30, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

- Step 7** Load the software image by entering the **tftp** command.

```
rommon #8> tftp
ROMMON Variable Settings:
ADDRESS=10.132.44.177
```

```
SERVER=10.129.0.30
GATEWAY=10.132.44.1
PORT=Ethernet0/0
VLAN=untagged
IMAGE=f1/asa800-232-k8.bin
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20

tftp f1/asa800-232-k8.bin@10.129.0.30 via 10.132.44.1

Received 14450688 bytes

Launching TFTP Image...
Cisco PIX Security Appliance admin loader (3.0) #0: Mon Mar  5 16:00:07 MST 2007

Loading...
```

After the software image is successfully loaded, the adaptive security appliance automatically exits ROMMOM mode.

- Step 8** To verify that the correct software image has been loaded into the adaptive security appliance, check the version in the adaptive security appliance by entering the following command:

```
hostname> show version
```

Erasing the Flash File System

- Step 1** Connect to the adaptive security appliance console port according to the instructions in [“Accessing the Command-Line Interface”](#) section on page 2-2.
- Step 2** Power off the adaptive security appliance, and then power it on.
- Step 3** During startup, press the **Escape** key when you are prompted to enter ROMMON mode.
- Step 4** To erase the file system, enter the **erase** command, which overwrites all files and erases the file system, including hidden system files.

```
rommon #1> erase [disk0: | disk1: | flash:]
```

Other Troubleshooting Tools

The adaptive security appliance provides other troubleshooting tools that you can use. This section includes the following topics:

- [Viewing Debug Messages, page 40-12](#)
- [Capturing Packets, page 40-12](#)
- [Viewing the Crash Dump, page 40-12](#)

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 less 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 ASA 5580 Adaptive 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 ASA 5580 Adaptive Security Appliance Command Reference](#).

Viewing the Crash Dump

If the adaptive 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 ASA 5580 Adaptive Security Appliance Command Reference](#).

Common Problems

This section describes common problems with the adaptive 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 current 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 or SSH connection to the adaptive security appliance interface.

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

Recommended Action Enable Telnet or SSH to the adaptive security appliance according to the instructions in “[Allowing Telnet Access](#)” section on page 37-1 or the “[Allowing SSH Access](#)” section on page 37-2.

Symptom You cannot ping the adaptive security appliance interface.

Possible Cause You disabled ICMP to the adaptive security appliance.

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

Symptom You cannot ping through the adaptive security appliance, although 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 adaptive 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 the 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 at the same security level.

Recommended Action Enable this feature according to the instructions in [“Allowing Communication Between Interfaces on the Same Security Level”](#) section on page 6-6.

