Troubleshooting Connections and Resources

This chapter describes how to troubleshoot the ASA and includes the following sections:

- Testing Your Configuration, page 1-1
- Monitoring Per-Process CPU Usage, page 1-7

Testing Your Configuration

This section describes how to test connectivity for the single mode ASA or for each security context, how to ping the ASA 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 debugging messages during troubleshooting. When you are done testing the ASA, follow the steps in the "Disabling the Test Configuration" section on page 1-6.

This section includes the following topics:

- Enabling ICMP Debugging Messages and Syslog Messages, page 1-2
- Pinging ASA Interfaces, page 1-3
- Passing Traffic Through the ASA, page 1-5
- Disabling the Test Configuration, page 1-6
- Determining Packet Routing with Traceroute, page 1-7
- Tracing Packets with Packet Tracer, page 1-7

Enabling ICMP Debugging Messages and Syslog Messages

Debugging messages and syslog messages can help you troubleshoot why your pings are not successful. The ASA only shows ICMP debugging messages for pings to the ASA interfaces, and not for pings through the ASA to other hosts.

To enable debugging and syslog messages, perform the following steps:

	Command	Purpose

Step 1	**`debug icmp trace`**
	Example:
	`hostname(config)# debug icmp trace`
		Shows ICMP packet information for pings to the ASA interfaces.

Step 2	**`logging monitor debug`**
	Example:
	`hostname(config)# logging monitor debug`
		Sets syslog messages to be sent to Telnet or SSH sessions.
		Note 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	**`terminal monitor`**
	Example:
	`hostname(config)# terminal monitor`
		Sends the syslog messages to a Telnet or SSH session.

Step 4	**`logging on`**
	Example:
	`hostname(config)# logging on`
		Enables syslog message generation.

Examples

The following example shows a successful ping from an external host (209.165.201.2) to the ASA 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 output 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 ASA Interfaces

To test whether the ASA interfaces are up and running and that the ASA and connected routers are operating correctly, you can ping the ASA interfaces.

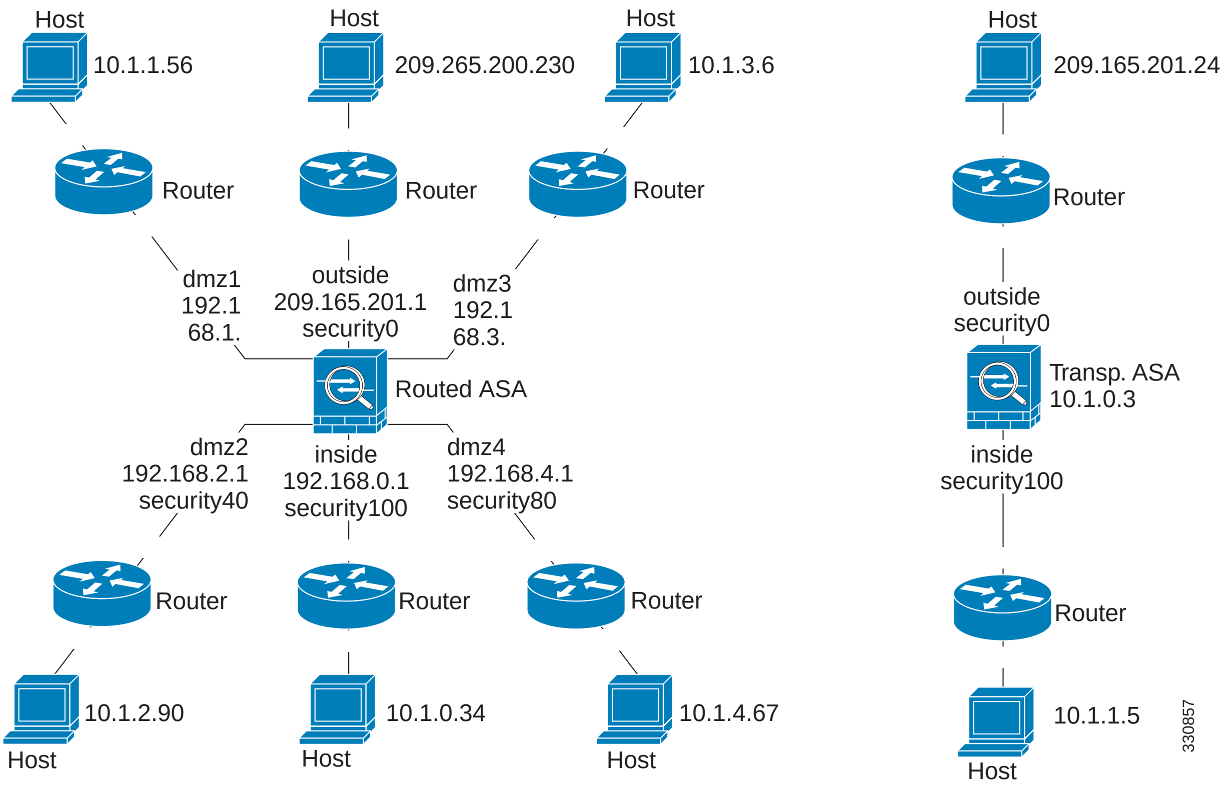
To ping the ASA interfaces, perform the following steps:

Step 1 Draw a diagram of your single-mode ASA 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 ASA. You will use this information in this procedure and in the procedure in the "Passing Traffic Through the ASA" section on page 1-5. (See Figure 1-1.)

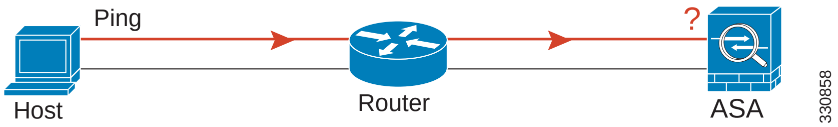
Figure 1-1 Network Diagram with Interfaces, Routers, and Hosts



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

A ping might fail if the ASA interface is not active, the interface configuration is incorrect, or if a switch between the ASA and a router is down (see Figure 1-2). In this case, no debugging messages or syslog messages appear, because the packet never reaches the ASA.

Figure 1-2 Ping Failure at the ASA Interface

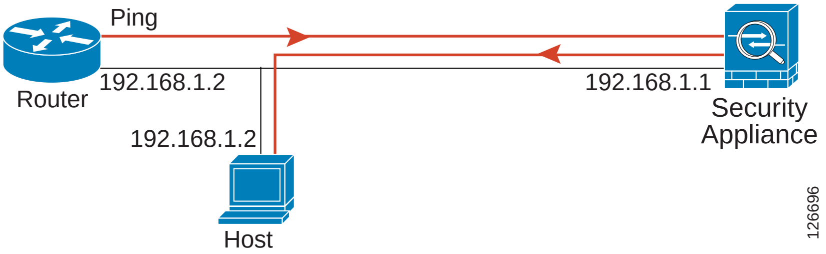


If the ping reaches the ASA, and it responds, debugging messages similar to the following appear:

```
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 1-3).

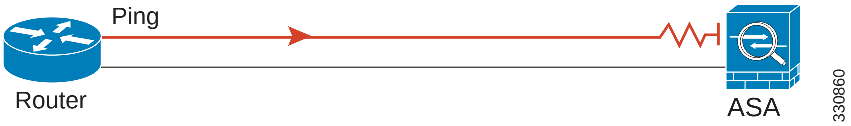
Figure 1-3 Ping Failure Because of IP Addressing Problems



Step 3 Ping each ASA 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 ASA, and whether the ASA can correctly route the packet back to the host.

A ping might fail if the ASA does not have a return route to the host through the intermediate router (see Figure 1-4). In this case, the debugging messages show that the ping was successful, but syslog message 110001 appears, indicating a routing failure has occurred.

Figure 1-4 Ping Failure Because the ASA Has No Return Route



Passing Traffic Through the ASA

After you successfully ping the ASA interfaces, make sure that traffic can pass successfully through the ASA. By default, you can ping from a high security interface to a low security interface. You just need to enable ICMP inspection to allow returning traffic through. If you want to ping from high to low, then you need to apply an ACL to allow traffic. If you use NAT, this test shows that NAT is operating correctly.

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.

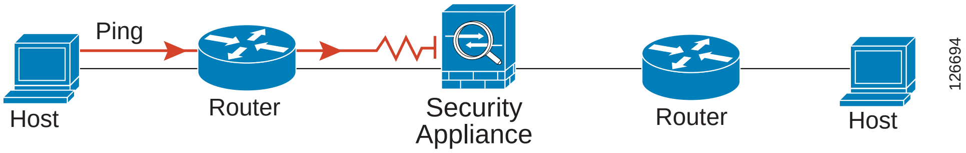
If the ping succeeds, a syslog message appears to confirm the address translation for routed mode (305009 or 305011) and that an ICMP connection was established (302020). You can also enter either the **show xlate** or **show conns** command to view this information.

The ping might fail because NAT is not configured correctly. In this case, a syslog 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, the following syslog message appears:

```
%ASA-3-106010: deny inbound icmp.
```

Note The ASA only shows ICMP debugging messages for pings to the ASA interfaces, and not for pings through the ASA to other hosts.

Figure 1-5 Ping Failure Because the ASA is Not Translating Addresses



Detailed Steps

	Command	Purpose
Step 1	`policy-map global_policy`	Edits the default global policy and enters policy-map configuration mode.
Step 2	`class inspection_default`	Edits the default class map, which matches application traffic for standard protocols and ports. For ICMP, this class matches all ICMP traffic.
Step 3	`inspect icmp`	Enables the ICMP inspection engine and ensures that ICMP responses can return to the source host.

Step 4	(Optional, for low security interfaces) `access-list ICMPACL extended permit icmp any any`	Adds an access list to allow ICMP traffic from any source host.
Step 5	`access-group ICMPACL in interface outside`	Assigns the access list to the outside interface. Replace “outside” with your interface name if it is different. Repeat the command for each interface that you want to allow ICMP traffic from high to low. **Note** After you apply this ACL to an interface that is not the lowest security interface, only ICMP traffic is allowed; the implicit permit from high to low is removed. For example, to allow a DMZ interface (level 50) to ping the inside interface (level 100), you need to apply this ACL. However, now traffic from DMZ to outside (level 0) is limited to ICMP traffic only, as opposed to all traffic that the implicit permit allowed before. After testing ping, be sure to remove this ACL from your interfaces, especially interfaces to which you want to restore the implicit permit (**no access-list ICMPACL**).

Disabling the Test Configuration

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

To disable the test configuration, perform the following steps:

	Command	Purpose
Step 1	`no debug icmp trace`	Disables ICMP debugging messages.
Step 2	`no logging on`	Disables logging.
Step 3	`no access-list ICMPACL`	Removes the ICMPACL access list, and deletes the related **access-group** commands.

Step 4	`policy-map global_policy`
	`  class inspection_default`
	`    no inspect icmp`
		(Optional) Disables the ICMP inspection engine.

Determining Packet Routing with 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 ASA.

Tracing Packets with Packet Tracer

The packet tracer tool provides packet tracing for packet sniffing and network fault isolation, as well as detailed information about the packets and how they are processed by the ASA. If a configuration command did not cause the packet to drop, the packet tracer tool can provide information about the cause in an easily readable format.

In addition, you can trace the lifespan of a packet through the ASA to see whether the packet is operating correctly with the packet tracer tool. This tool enables you to 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.
- Search for an IPv4 or IPv6 address based on the user identity and the FQDN.

To trace packets, enter the following command:

Command	Purpose
packet-tracer input [*ifc_name*] [**icmp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *type code ident* [*dip* | **fqdn** *fqdn-string*]] | [**tcp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *sport* [*dip* | **fqdn** *fqdn-string*] *dport*] | [**udp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *sport* [*dip* | **fqdn** *fqdn-string*] *dport*] | [**rawip** [*sip* | **user** *username* | **fqdn** *fqdn-string*] [*dip* | **fqdn** *fqdn-string*]] [**detailed**] [**xml**] **Example:** `hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed`	Provides detailed information about the packets and how they are processed by the ASA. The example shows how to enable packet tracing from inside host 10.2.25.3 to external host 209.165.202.158, including detailed information.

Monitoring Per-Process CPU Usage

You can monitor the processes that run on the CPU. You can obtain information about the percentage of CPU that is used by a certain process. CPU usage statistics are sorted in descending order to display the highest consumer at the top. Also included is information about the load on the CPU per process, at 5 seconds, 1 minute, and 5 minutes before the log time. This information is updated automatically every 5 seconds to provide real-time statistics.

You can use the **show process cpu-usage sorted** command to find a breakdown of the process-related load-to-CPU that is consumed by any configured contexts.