Troubleshooting

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

- Testing Your Configuration, page 81-1
- Other Troubleshooting Tools, page 81-8
- Common Problems, page 81-17
- Additional Troubleshooting, page 81-18

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.

This section includes the following topics:

- Pinging ASA Interfaces, page 81-1
- Passing Traffic Through the ASA, page 81-3
- Verifying ASA Configuration and Operation, and Testing Interfaces Using Ping, page 81-3
- Determining Packet Routing with Traceroute, page 81-6
- Tracing Packets with Packet Tracer, page 81-7

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.
Testing Your Configuration

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 81-3. (See Figure 81-1.)

Figure 81-1  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 81-2). In this case, no debug messages or syslog messages appear, because the packet never reaches the ASA.

Figure 81-2  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 81-3).
Figure 81-3 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 81-4). In this case, the debugging messages show that the ping was successful, but syslog message 110001 appears, indicating a routing failure.

Figure 81-4 Ping Failure Because the Security Appliance 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. 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 ASA is operating correctly. If the ping fails in transparent mode, contact the Cisco TAC.

Verifying ASA Configuration and Operation, and Testing Interfaces Using Ping

The Ping tool is useful for verifying the configuration and operation of the ASA and surrounding communications links, as well as for testing other network devices.

This section includes the following topics:

- Pinging From an ASA Interface, page 81-4
- Pinging to an ASA Interface, page 81-4
- Pinging Through the ASA Interface, page 81-4
- Troubleshooting the Ping Tool, page 81-5
- Using the Ping Tool, page 81-5

A ping is sent to an IP address and it returns a reply. This process enables network devices to discover, identify, and test each other.
The Ping tool uses ICMP (as described in RFC 777 and RFC 792) to define an echo request-and-reply transaction between two network devices. The echo request packet is sent to the IP address of a network device. The receiving device reverses the source and destination address and sends the packet back as the echo reply.

Administrators can use the ASDM Ping interactive diagnostic tool in these ways:

- Loopback testing of two interfaces—A ping may be initiated from one interface to another on the same ASA, as an external loopback test to verify basic “up” status and operation of each interface.
- Pinging to an ASA—The Ping tool can ping an interface on another ASA to verify that it is up and responding.
- Pinging through an ASA—Ping packets originating from the Ping tool may pass through an intermediate ASA on their way to a device. The echo packets will also pass through two of its interfaces as they return. This procedure can be used to perform a basic test of the interfaces, operation, and response time of the intermediate unit.
- Pinging to test questionable operation of a network device—A ping may be initiated from an ASA interface to a network device that is suspected of functioning incorrectly. If the interface is configured correctly and an echo is not received, there may be problems with the device.
- Pinging to test intermediate communications—A ping may be initiated from an ASA interface to a network device that is known to be functioning correctly and returning echo requests. If the echo is received, the correct operation of any intermediate devices and physical connectivity is confirmed.

**Pinging From an ASA Interface**

For basic testing of an interface, you can initiate a ping from an ASA interface to a network device that you know is functioning correctly and returning replies through the intermediate communications path. For basic testing, make sure you do the following:

- Verify receipt of the ping from the ASA interface by the “known good” device. If the ping is not received, a problem with the transmitting hardware or interface configuration may exist.
- If the ASA interface is configured correctly and it does not receive an echo reply from the “known good” device, problems with the interface hardware receiving function may exist. If a different interface with “known good” receiving capability can receive an echo after pinging the same “known good” device, the hardware receiving problem of the first interface is confirmed.

**Pinging to an ASA Interface**

When you try to ping to an ASA interface, verify that the pinging response (ICMP echo reply) is enabled for that interface by choosing Tools > Ping. When pinging is disabled, the ASA cannot be detected by other devices or software applications, and does not respond to the ASDM Ping tool.

**Pinging Through the ASA Interface**

To verify that other types of network traffic from “known good” sources are being passed through the ASA, choose Monitoring > Interfaces > Interface Graphs or an SNMP management station.

To enable internal hosts to ping external hosts, configure ICMP access correctly for both the inside and outside interfaces, choose Configuration > Firewall > Objects > IP Names.
Troubleshooting the Ping Tool

When pings fail to receive an echo, it may be the result of a configuration or operational error in an ASA, and not necessarily because of no response from the IP address being pinged. Before using the Ping tool to ping from, to, or through an ASA interface, perform the following basic checks:

- Verify that interfaces are configured. Choose Configuration > Device Setup > Interfaces.
- Verify that devices in the intermediate communications path, such as switches or routers, are correctly delivering other types of network traffic.
- Make sure that traffic of other types from “known good” sources is being passed. Choose Monitoring > Interfaces > Interface Graphs.

Using the Ping Tool

To use the Ping tool, perform the following steps:

**Step 1**
In the main ASDM application window, choose Tools > Ping.
The Ping dialog box appears.

**Step 2**
Enter the destination IP address for the ICMP echo request packets in the IP Address field.
Ping can also accept IPv6 addresses.

**Note**
If a hostname has been assigned in the Configuration > Firewall > Objects > IP Names pane, you can use the hostname in place of the IP address.

**Step 3**
(Optional) Choose the ASA interface that transmits the echo request packets from the drop-down list. If it is not specified, the ASA checks the routing table to find the destination address and uses the required interface.

**Step 4**
Click Ping to send an ICMP echo request packet from the specified or default interface to the specified IP address and start the response timer.
The response appears in the Ping Output area. Three attempts are made to ping the IP address, and results display the following fields:

- The IP address of the device pinged or a device name, if available. The name of the device, if assigned Hosts/Networks, may be displayed, even if NO response is the result.
- When the ping is transmitted, a millisecond timer starts with a specified maximum, or timeout value. This timer is useful for testing the relative response times of different routes or activity levels.

**Example Ping output:**

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

**Step 5**
To enter a new IP address, click Clear Screen to remove the previous response from the Ping output area.
Determining Packet Routing with Traceroute

The Traceroute tool helps you to determine the route that packets will take to their destination. The tool prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following table lists the output symbols printed by this tool.

<table>
<thead>
<tr>
<th>Output Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>No response was received for the probe within the timeout period.</td>
</tr>
<tr>
<td>nn msec</td>
<td>For each node, the round-trip time (in milliseconds) for the specified number of probes.</td>
</tr>
<tr>
<td>!N</td>
<td>ICMP network unreachable.</td>
</tr>
<tr>
<td>!H</td>
<td>ICMP host unreachable.</td>
</tr>
<tr>
<td>!P</td>
<td>ICMP unreachable.</td>
</tr>
<tr>
<td>!A</td>
<td>ICMP administratively prohibited.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown ICMP error.</td>
</tr>
</tbody>
</table>

To use the Traceroute tool, perform the following steps:

1. In the main ASDM application window, choose **Tools > Traceroute**.
2. Enter the name of the host to which the route is traced. If the hostname is specified, define it by choosing **Configuration > Firewall > Objects > IP Names**, or configure a DNS server to enable this tool to resolve the hostname to an IP address.
3. Enter the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.
4. Type the destination port used by the UDP probe messages. The default is 33434.
5. Enter the number of probes to be sent at each TTL level. The default is three.
6. Specify the minimum and maximum TTL values for the first probes. The minimum default is one, but it can be set to a higher value to suppress the display of known hops. The maximum default is 30. The traceroute terminates when the packet reaches the destination or when the maximum value is reached.
7. Check the **Specify source interface or IP address** check box. Choose the source interface or IP address for the packet trace from the drop-down list. This IP address must be the IP address of one of the interfaces. In transparent mode, it must be the management IP address of the ASA.
8. Check the **Reverse Resolve** check box to have the output display the names of hops encountered if name resolution is configured. Leave this check box unchecked to have the output display IP addresses.
9. Check the **Use ICMP** check box to specify the use of ICMP probe packets instead of UDP probe packets.
10. Click **Trace Route** to start the traceroute.
11. Click **Clear Output** to start a new traceroute.
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 provides information about the cause in an easily readable manner.

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 open the packet tracer, perform the following steps:

**Step 1** In the main ASDM application window, choose **Tools > Packet Tracer**.

The Cisco ASDM Packet Tracer dialog box appears.

**Step 2** Choose the source interface for the packet trace from the drop-down list.

**Step 3** Specify the protocol type for the packet trace. Available protocol types include ICMP, IP, TCP, and UDP.

**Step 4** Enter the source IP address for the packet trace in the Source IP Address field.

**Step 5** For TCP and UDP only, choose the source port for the packet trace from the drop-down list.

**Step 6** Enter the destination IP address for the packet trace in the Destination IP Address field.

**Step 7** For TCP and UDP only, choose the destination port for the packet trace from the drop-down list.

**Step 8** For ICMP only, choose the type of packet trace from the Type drop-down list. Then enter the trace code and trace ID in the appropriate fields.

**Step 9** For IP only, enter the protocol number in the Protocol field. Valid values range from 0 to 255.

**Step 10** Click **Start** to trace the packet.

The Information Display Area shows detailed messages about the results of the packet trace.

**Note** To display a graphical representation of the packet trace, check the **Show animation** check box.

**Step 11** Click **Clear** to start a new packet trace.

Handling TCP Packet Loss

To troubleshoot TCP packet loss, see the “Customizing the TCP Normalizer with a TCP Map” section on page 57-6 for more information.
Other Troubleshooting Tools

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

- Configuring and Running Captures with the Packet Capture Wizard, page 81-8
- Sending an Administrator’s Alert to Clientless SSL VPN Users, page 81-11
- Saving an Internal Log Buffer to Flash, page 81-12
- Viewing and Copying Logged Entries with the ASDM Java Console, page 81-12
- Monitoring Performance, page 81-12
- Monitoring System Resources, page 81-13
- Monitoring Connections, page 81-16
- Monitoring Per-Process CPU Usage, page 81-16

Configuring and Running Captures with the Packet Capture Wizard

You can use the Packet Capture Wizard to configure and run captures for troubleshooting errors. The captures can use access lists to limit the type of traffic captured, the source and destination addresses and ports, and one or more interfaces. The wizard runs one capture on each of the ingress and egress interfaces. You can save the captures on your PC to examine them in a packet analyzer.

**Note**
This tool does not support clientless SSL VPN capture.

To configure and run captures, perform the following steps:

**Step 1**
In the main ASDM application window, choose **Wizards > Packet Capture Wizard**.

The Overview of Packet Capture screen appears, with a list of the tasks through which the wizard will guide you to complete.

**Step 2**
Click **Next** to display the Ingress Traffic Selector screen.

**Step 3**
Choose the ingress interface from the drop-down list.

**Step 4**
In the Packet Match Criteria area, do one of the following:

- To specify the access list to use for matching packets, click the **Specify access-list** radio button, and then choose the access list from the Select access list drop-down list. To add a previously configured access list to the current drop-down list, click **Manage** to display the ACL Manager pane. Choose an access list, and click **OK**.
- To specify packets parameters, click the **Specify Packet Parameters** radio button.

**Step 5**
Click **Next** to display the Ingress Traffic Selector screen. For more information, see the “Ingress Traffic Selector” section on page 81-10.

**Step 6**
Enter the source host IP address and choose the network IP address from the drop-down list.

**Step 7**
Enter the destination host IP address and choose the network IP address from the drop-down list.

**Step 8**
Choose the protocol type to capture from the drop-down list. Available protocol types to capture are ah, eigrp, esp, gre, icmp, icmp6, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, snp, tcp, or udp.
Step 9  Click **Next** to display the Egress Traffic Selector screen. For more information, see the “Egress Traffic Selector” section on page 81-10.

Step 10  Choose the egress interface from the drop-down list.

Step 11  Enter the source host IP address and choose the network IP address from the drop-down list.

Step 12  Enter the destination host IP address and choose the network IP address from the drop-down list.

*Note*  The source port services, destination port services, and ICMP type are read-only and are based on the choices that you made in the Ingress Traffic Selector screen.

Step 13  Click **Next** to display the Buffers & Captures screen. For more information, see the “Buffers” section on page 81-10.

Step 14  In the Capture Parameters area, to obtain the latest capture every 10 seconds automatically, check the **Get capture every 10 seconds** check box. By default, this capture uses the circular buffer.

Step 15  In the Buffer Parameters area, you specify the buffer size and packet size. The buffer size is the maximum amount of memory that the capture can use to store packets. The packet size is the longest packet that the capture can hold. We recommend that you use the longest packet size to capture as much information as possible.

a. Enter the packet size. The valid size ranges from 14 - 1522 bytes.
b. Enter the buffer size. The valid size ranges from 1534 - 33554432 bytes.
c. Check the **Use circular buffer** check box to store captured packets.

*Note*  When you choose this setting, if all the buffer storage is used, the capture starts overwriting the oldest packets.

Step 16  Click **Next** to display the Summary screen, which shows the traffic selectors and buffer parameters that you have entered. For more information, see the “Summary” section on page 81-11.

Step 17  Click **Next** to display the Run Captures screen, and then click **Start** to begin capturing packets. Click **Stop** to end the capture. For more information, see the “Run Captures” section on page 81-11.

Step 18  Click **Get Capture Buffer** to determine how much buffer space you have remaining. Click **Clear Buffer on Device** to remove the current content and allow room in the buffer to capture more packets.

Step 19  Click **Save captures** to display the Save Capture dialog box. Choose the format in which you want to include the captures: **ASCII** or **PCAP**. You have the option of saving either the ingress capture, the egress capture, or both.

Step 20  To save the ingress packet capture, click **Save Ingress Capture** to display the Save capture file dialog box. Specify the storage location on your PC, and click **Save**.

Step 21  Click **Launch Network Sniffer Application** to start the packet analysis application specified in Tools > Preferences for analyzing the ingress capture.

Step 22  To save the egress packet capture, click **Save Egress Capture** to display the Save capture file dialog box. Specify the storage location on your PC, and click **Save**.

Step 23  Click **Launch Network Sniffer Application** to start the packet analysis application specified in Tools > Preferences for analyzing the egress capture.

Step 24  Click **Close**, and then click **Finish** to exit the wizard.
Ingress Traffic Selector

To configure the ingress interface, source and destination hosts/networks, and the protocol for packet capture, perform the following steps:

**Step 1** Enter the ingress interface name.

**Step 2** Enter the ingress source host and network.

**Step 3** Enter the ingress destination host and network.

**Step 4** Enter the protocol type to capture. Available protocols are ah, eigrp, esp, gre, icmp, icmp6, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, snp, tcp, or udp.
   a. Enter the ICMP type for ICMP only. Available types include all, alternate address, conversion-error, echo, echo-reply, information-reply, information-request, mask-reply, mask-request, mobile-redirect, parameterProblem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-reply, timestamp-request, traceroute, or unreachable.
   b. Specify the source and destination port services for the TCP and UDP protocols only. Available options include the following:
      – To include all services, choose All Services.
      – To include a service group, choose Service Groups.
      – To include a specific service, choose one of the following: aol, bgp, chargen, cifx, citrix-ica, ctiqbe, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, https, ident, imap4, irc, kerberos, klogin, kshell, ldap, ldaps, login, lotusnotes, lpd, netbios-ssn, nntp, pcanywhere-data, pim-auto-rp, pop2, pop3, pptp, rsh, rtsp, sip, smtp, sqlnet, ssh, sunrpc, tacacs, talk, telnet, uucp, or whois.

Egress Traffic Selector

To configure the egress interface, source and destination hosts/networks, and source and destination port services for packet capture, perform the following steps:

**Step 1** Enter the egress interface name.

**Step 2** Enter the egress source host and network.

**Step 3** Enter the egress destination host and network.

The protocol type selected during the ingress configuration is already listed.

Buffers

To configure the packet size, buffer size, and use of the circular buffer for packet capture, perform the following steps:

**Step 1** Enter the longest packet that the capture can hold. Use the longest size available to capture as much information as possible.

**Step 2** Enter the maximum amount of memory that the capture can use to store packets.
Step 3 Use the circular buffer to store packets. When the circular buffer has used all of the buffer storage, the capture will overwrite the oldest packets first.

Summary

The Summary screen shows the traffic selectors and the buffer parameters for the packet capture selected in the previous wizard screens.

Run Captures

To start and stop the capture session, view the capture buffer, launch a network analyzer application, save packet captures, and clear the buffer, perform the following steps:

Step 1 To begin the packet capture session on a selected interface, click Start.
Step 2 To stop the packet capture session on a selected interface, click Stop.
Step 3 To obtain a snapshot of the captured packets on the interface, click Get Capture Buffer.
Step 4 To show the capture buffer on the ingress interface, click Ingress.
Step 5 To show the capture buffer on the egress interface, click Egress.
Step 6 To clear the buffer on the device, click Clear Buffer on Device.
Step 7 To start the packet analysis application for analyzing the ingress capture or the egress capture specified in Tools > Preferences, click Launch Network Sniffer Application.
Step 8 To save the ingress and egress captures in either ASCII or PCAP format, click Save Captures.

Save Captures

To save the ingress and egress packet captures to ASCII or PCAP file format for further packet analysis, perform the following steps:

Step 1 To save the capture buffer in ASCII format, click ASCII.
Step 2 To save the capture buffer in PCAP format, click PCAP.
Step 3 To specify a file in which to save the ingress packet capture, click Save ingress capture.
Step 4 To specify a file in which to save the egress packet capture, click Save egress capture.

Sending an Administrator’s Alert to Clientless SSL VPN Users

To send an alert message to clientless SSL VPN users (for example, about connection status), perform the following steps:
**Other Troubleshooting Tools**

---

**Step 1**
In the main ASDM application window, choose **Tools > Administrator’s Alert Message to Clientless SSL VPN Users**.

The Administrator’s Alert Message to Clientless SSL VPN Users dialog box appears.

**Step 2**
Enter the new or edited alert content that you want to send, and then click **Post Alert**.

**Step 3**
To remove current alert content and enter new alert content, click **Cancel Alert**.

---

**Saving an Internal Log Buffer to Flash**

To save the internal log buffer to flash memory, perform the following steps:

**Step 1**
In the main ASDM application window, choose **File > Save Internal Log Buffer to Flash**.

The Enter Log File Name dialog box appears.

**Step 2**
Choose the first option to save the log buffer with the default filename, LOG-YYYY-MM-DD-hhmmss.txt.

**Step 3**
Choose the second option to specify a filename for the log buffer.

**Step 4**
Enter the filename for the log buffer, and then click **OK**.

---

**Viewing and Copying Logged Entries with the ASDM Java Console**

You can use the ASDM Java console to view and copy logged entries in a text format, which can help you troubleshoot ASDM errors.

To access the ASDM Java Console, perform the following steps:

**Step 1**
In the main ASDM application window, choose **Tools > ASDM Java Console**.

**Step 2**
To show the virtual machine memory statistics, enter **m** in the console.

**Step 3**
To perform garbage collection, enter **g** in the console.

**Step 4**
To monitor memory usage, open the Windows Task Manager and double-click the **asdm_launcher.exe** file.

**Note**
The maximum memory allocation allowed is 256 MB.

---

**Monitoring Performance**

To view ASA performance information in a graphical or tabular format, perform the following steps:

**Step 1**
In the ASDM main window, choose **Monitoring > Properties > Connection Graphs > Perfmon**.
Step 2 Select one or more entries from the Available Graphs list, then click Add to move them to the Selected Graphs list. To remove an entry from the Selected Graphs list, click Remove. The available options are the following:

- AAA Perfmon—Displays the ASA AAA performance information.
- Inspection Perfmon—Displays the ASA inspection performance information.
- Web Perfmon—Displays the ASA web performance information, including URL access and URL server requests.
- Connections Perfmon—Displays the ASA connections performance information.
- Xlate Perfmon—Displays the ASA NAT performance information.

You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Step 3 To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title in the Graph Window Title field.

Step 4 Click Show Graphs to view performance statistics in a new or updated graph window.

Step 5 Click the Table tab to view the same performance statistics in a tabular format.

Step 6 From the View drop-down list on either tab, choose to display updates to information in the following time periods: Real-time, data every 10 sec; Last 10 minutes, data every 10 sec; Last 60 minutes, data every 1 min; Last 12 hours, data every 12 minutes; or Last 5 days, data every two hours.

Step 7 (Optional) Click Export to display the Export Graph Data dialog box. The selected performance statistics to export are already checked.

Step 8 (Optional) Click Export again to display the Save dialog box.

Step 9 (Optional) Click Save to save the performance statistics to a text file (.txt) on your local drive for future reference.

Step 10 (Optional) Click Print to display the Print Graph dialog box.

Step 11 (Optional) Choose the graph or table name from the drop-down list, then click Print to display the Print dialog box.

Step 12 (Optional) Click OK to print the selected performance statistics.

Monitoring System Resources

This section includes the following topics:

- Blocks, page 81-13
- CPU, page 81-14
- Memory, page 81-15

Blocks

To view the free and used memory blocks, perform the following steps:

Step 1 In the ASDM main window, choose Monitoring > Properties > System Resources Graphs > Blocks.
Step 2 Select one or more entries from the Available Graphs list, then click Add to move them to the Selected Graphs list. To remove an entry from the Selected Graphs list, click Remove. The available options are the following:

- Blocks Used—Displays the ASA used memory blocks.
- Blocks Free—Displays the ASA free memory blocks.

You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Step 3 To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title in the Graph Window Title field.

Step 4 Click Show Graphs to view system resource statistics in a new or updated graph window.

Step 5 Click the Table tab to view the same performance statistics in a tabular format.

Step 6 From the View drop-down list on either tab, choose to display updates to information in the following time periods: Real-time, data every 10 sec; Last 10 minutes, data every 10 sec; Last 60 minutes, data every 1 min; Last 12 hours, data every 12 minutes; or Last 5 days, data every two hours.

Step 7 (Optional) Click Export to display the Export Graph Data dialog box. The selected memory block statistics to export are already checked.

Step 8 (Optional) Click Export again to display the Save dialog box.

Step 9 (Optional) Click Save to save the memory block statistics to a text file (.txt) on your local drive for future reference.

Step 10 (Optional) Click Print to display the Print Graph dialog box.

Step 11 (Optional) Choose the graph or table name from the drop-down list, then click Print to display the Print dialog box.

Step 12 (Optional) Click OK to print the selected memory block statistics.

---

CPU

To view the CPU utilization, perform the following steps:

Step 1 In the ASDM main window, choose Monitoring > Properties > System Resources Graphs > CPU.

Step 2 Select one or more entries from the Available Graphs list, then click Add to move them to the Selected Graphs list. To remove an entry from the Selected Graphs list, click Remove.

You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Step 3 To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title in the Graph Window Title field.

Step 4 Click Show Graphs to view system resource statistics in a new or updated graph window.

Step 5 Click the Table tab to view the same performance statistics in a tabular format.

Step 6 From the View drop-down list on either tab, choose to display updates to information in the following time periods: Real-time, data every 10 sec; Last 10 minutes, data every 10 sec; Last 60 minutes, data every 1 min; Last 12 hours, data every 12 minutes; or Last 5 days, data every two hours.

Step 7 (Optional) Click Export to display the Export Graph Data dialog box. The selected CPU utilization statistics to export are already checked.
### Memory

To view the memory utilization, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the ASDM main window, choose Monitoring &gt; Properties &gt; System Resources Graphs &gt; Blocks.</td>
</tr>
</tbody>
</table>
| Step 2 | Select one or more entries from the Available Graphs list, then click Add to move them to the Selected Graphs list. To remove an entry from the Selected Graphs list, click Remove. The available options are the following:  
  - Free Memory—Displays the ASA free memory.  
  - Used Memory—Displays the ASA used memory.  
You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time. |
| Step 3 | To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title in the Graph Window Title field. |
| Step 4 | Click Show Graphs to view system resource statistics in a new or updated graph window. |
| Step 5 | Click the Table tab to view the same performance statistics in a tabular format. |
| Step 6 | From the View drop-down list on either tab, choose to display updates to information in the following time periods: Real-time, data every 10 sec; Last 10 minutes, data every 10 sec; Last 60 minutes, data every 1 min; Last 12 hours, data every 12 minutes; or Last 5 days, data every two hours. |
| Step 7 | (Optional) Click Export to display the Export Graph Data dialog box. The selected memory utilization statistics to export are already checked. |
| Step 8 | (Optional) Click Export again to display the Save dialog box. |
| Step 9 | (Optional) Click Save to save the memory utilization statistics to a text file (.txt) on your local drive for future reference. |
| Step 10 | (Optional) Click Print to display the Print Graph dialog box. |
| Step 11 | (Optional) Choose the graph or table name from the drop-down list, then click Print to display the Print dialog box. |
| Step 12 | (Optional) Click OK to print the selected memory utilization statistics. |
Monitoring Connections

To view current connections in a tabular format, in the ASDM main window, choose Monitoring > Properties > Connections. Each connection is identified by the following parameters:

- Protocol
- Source IP address
- Source port
- Destination IP address
- Destination port
- Idle time since the last packet was sent or received
- Amount of sent and received traffic on the connection

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. In ASDM it is updated every 30 seconds.

To view CPU usage on a per-process basis, perform the following steps:

Step 1  In the ASDM main window, choose Monitoring > Properties > Per-Process CPU Usage.

Step 2  To pause the auto-refresh of the screen, click Stop auto-refresh.

Step 3  To save the information on the screen to a local text file, click Save log to local file.

The Save dialog box appears.

Step 4  Enter the name of the text file, then click Save.

To color code processes according to their CPU usage range, click Configure CPU usage.

The Color Settings dialog box appears.

Step 5  Choose one of the following range options: 49% and below, 50% to 79%, and 80% and above.

Step 6  Click the foreground or background cell to display the Pick a Color dialog box, and select the foreground and background colors for the given ranges.

Step 7  Click one of the following tabs to pick the color palette: Swatches, HSB, or RGB. When you are done, click OK.

Step 8  Click OK to view the color-coded entries.

Step 9  Click Refresh to refresh the data manually at any time.
Common Problems

This section describes common problems with the ASA, 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 start run command. Load the startup configuration as your active configuration. Then change the password and then enter 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 ASA interface.

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

Recommended Action  Enable Telnet or SSH to the ASA according to the instructions in the “Configuring ASA Access for ASDM, Telnet, or SSH” section on page 40-1.

Symptom  You cannot ping the ASA interface.

Possible Cause  You disabled ICMP to the ASA.

Recommended Action  Enable ICMP to the ASA for your IP address using the icmp command.

Symptom  You cannot ping through the ASA, 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 ASA 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 the “Allowing Same Security Level Communication” section on page 14-21.
Symptom  IPsec tunnels do not duplicate during a failover to the standby device.

Possible Cause  The switch port that the ASA is plugged into is set to 10/100 instead of 1000.

Recommended Action  Set the switch port that the ASA is plugged into to 1000.

Additional Troubleshooting

This section includes additional information about troubleshooting your ASA.

Maximum configuration size—ASDM supports a maximum configuration size of 512 KB. If you exceed this amount you may experience performance issues. For example, when you load the configuration, the status dialog shows the percentage of the configuration that is complete, yet with large configurations it stops incrementing and appears to suspend operation, even though ASDM might still be processing the configuration. If this situation occurs, we recommend that you consider increasing the ASDM system heap memory.

To increase the ASDM heap memory size, modify the launcher shortcut by performing the following procedure:

---

Step 1 Right-click the shortcut for the ASDM-IDM Launcher, and choose Properties.

Step 2 Choose the Shortcut tab.

Step 3 In the Target field, change the argument prefixed with "-Xmx" to specify your desired heap size. For example, change it to -Xmx768m for 768 MB or -Xmx1g for 1 GB. For more information about this parameter, see the Oracle document in the following location:
http://docs.oracle.com/javase/1.5.0/docs/tooldocs/windows/java.html