



CHAPTER 47

Monitoring Properties

This chapter contains the following topics:

- [AAA Servers](#)
- [Device Access](#)
- [Connection Graphs](#)
- [Connection Graphs](#)
- [DNS Cache](#)
- [IP Audit](#)
- [System Resources Graphs](#)
- [WCCP](#)

AAA Servers

This pane allows you to view and refresh AAA server statistics.

Fields

- **Server Group**—Displays a configured server group, or LOCAL if none have been configured.
- **Protocol**—Displays what protocol the server group uses for AAA.
- **IP Address**—Displays the IP address of the configured AAA server.
- **Status**—Displays the status (Active or Inactive) of the configured AAA server.

Below the list of AAA servers are the statistics for each configured server. You can clear the statistics by clicking **Clear Server Statistics**. You can refresh the server status by clicking **Update Server Status**

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Device Access

This pane lets you monitor management sessions, AAA locked out users, and authenticated users. This section includes the following topics:

- [AAA Local Locked Out Users](#)
- [Authenticated Users](#)
- [ASDM/HTTPS Sessions](#)
- [Secure Shell Sessions](#)
- [Telnet Sessions](#)

AAA Local Locked Out Users

The AAA Local Locked Out Users pane lets you view a list of users who have been locked out of ASDM because of failed login attempts. You can also clear selected lockout conditions or all lockouts.

Fields

- **Currently locked out users**—Displays a list of the currently locked out users.
- **Lock Time**—Specifies the amount of time that the user has been locked out of the system.
- **Failed Attempts**—Specifies the number of failed login attempts.
- **User**—The user name identified with the failed login attempts.
- **Clear lockout**—Click to clear the selected user lockout condition.
- **Clear all lockouts**—Click to clear all user lockout conditions. It is good practice to refresh the list of lockout conditions before clearing all lockouts.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Authenticated Users

This pane lets you view which users have been authenticated to use the security appliance. Each row represents one user.

Fields

- **User**—Displays the username of the person authenticated to use the security appliance.
- **IP Address**—Displays the IP address of the user authenticated to use the security appliance.
- **Dynamic ACL**—Displays the dynamic access list of the user authenticated to use the security appliance.

- Inactivity Timeout—Displays the amount of time that the selected user must remain inactive before the session times out and the user is disconnected.
- Absolute Timeout—Displays the amount of time that the selected user can remain connected before the session closes and the user is disconnected.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

ASDM/HTTPS Sessions

The ASDM/HTTPS pane lets you view currently connected ASDM/HTTPS sessions.

Fields

- Session ID—Displays the name of a connected ASDM/HTTPS session.
- IP Address—Displays the IP address of each host or network that is allowed to connect to this security appliance.
- Disconnect—Select to disconnect a connected ASDM/HTTPS session.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Secure Shell Sessions

The Secure Shell Sessions pane lets you view hosts connected to the security appliance for administrative access using the SSH protocol.

Fields

- Client—Displays the client type for the selected SSH session.
- User—Displays the user name for the selected SSH session.
- State—Displays the state of the selected SSH session.
- Version—Displays the version of SSH used to connect to the security appliance.
- Encryption (in)—Displays the inbound encryption method used for the selected session.

- Encryption (out)—Displays the outbound encryption method used for the selected session.
- HMAC (in)—Displays the configured HMAC for the selected inbound SSH session.
- HMAC (out)—Displays the configured HMAC for the selected outbound SSH session.
- SID—Displays the secure ID of the selected session.
- Disconnect—Click to disconnect a connected SSH session.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Telnet Sessions

The Telnet Sessions pane lets you view currently connected Telnet sessions.

Fields

- Session ID—Displays the name of a connected Telnet session.
- IP Address—Displays the IP address of each host that is allowed to connect to this security appliance over Telnet.
- Disconnect—Click to disconnect a connected Telnet session.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Connection Graphs

The Connection Graphs pane lets you view connection information about the security appliance in graph format. You can view information about NAT and performance monitoring information, including UDP connections, AAA performance, and inspection information. This section includes the following topics:

- [Perfmon](#)
- [Xlates](#)

Perfmon

The Perfmon pane lets you view the performance information in a graphical format. 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.

Fields

- Available Graphs—Lists the components you can graph.
 - AAA Perfmon—Displays the security appliance AAA performance information.
 - Inspection Perfmon—Displays the security appliance inspection performance information.
 - Web Perfmon—Displays the security appliance web performance information, including URL access and URL server requests.
 - Connections Perfmon—Displays the security appliance connections performance information.
 - Xlate Perfmon—Displays the security appliance NAT performance information.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. 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.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected statistic type from the Selected Graphs field.
- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Xlates

This pane lets you view the active Network Address Translations in a graphical format. 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.

Fields

- Available Graphs—Lists the components you can graph.
 - Xlate Utilization—Displays the security appliance NAT utilization.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. 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.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected entry from the Selected Graphs list.

- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

CRL

This pane allows you to view or clear associated CRLs of selected CA certificates.

Fields

- CA Certificate Name—Choose the name of the selected certificate from the drop-down list.
- View CRL—Click to view the selected CRL.
- Clear CRL—Click to clear the selected CRL from the cache.
- CRL Info—*Display only*. Displays detailed CRL information.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DNS Cache

The security appliance provides a local cache of DNS information from external DNS queries that are sent for certain clientless SSL VPN and certificate commands. Each DNS translation request is first looked for in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache can not resolve the request, a DNS query is sent to the various DNS servers that have been configured. If an external DNS server resolves the request, the resulting IP address is stored in the local cache along with its corresponding hostname.

Important Notes

- DNS cache entries are time stamped. The time stamp will be used to age out unused entries. When the entry is added to the cache, the time stamp is initialized. Each time the entry is accessed, the timestamp is updated. At a configured time interval, the DNS cache will check all entries and purge those entries whose time exceeds a configured age-out timer.

- If new entries arrive but there is no room in the cache because the size was exceeded or no more memory is available, the cache will be thinned by one third, based on the entries age. The oldest entries will be removed.

Fields

- Host— Shows the DNS name of the host.
- IP Address—Shows the address that resolves to the hostname.
- Permanent—Indicates whether the entry was made through a **name** command.
- Idle Time—Specifies the time elapsed since the security appliance last referred to that entry.
- Active—Indicates whether the entry has aged out. If there is not adequate space in cache, this entry may be deleted.
- Clear Cache—Click to clear the entire DNS cache.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	—

IP Audit

The IP Audit pane lets you view the number of packets that match informational and attack signatures that are shown in graphical or tabular form. Each graph type shows the combined packets for all interfaces that have this feature enabled.

Fields

- Available Graphs—Lists the types of signatures available for monitoring. See [IP Audit Signatures](#) for detailed information about each signature type. 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.
 - IP Options—Shows the packet count for the following signatures:
 - Bad Options List (1000)
 - Timestamp (1002)
 - Provide s, c, h, tcc (1003)
 - SATNET ID (1005)
 - IP Route Options—Shows the packet count for the following signatures:
 - Loose Source Route (1004)
 - Record Packet Route (1001)
 - Strict Source Route (1006)
 - IP Attacks—Shows the packet count for the following signatures:
 - IP Fragment Attack (1100)

- Impossible IP Packet (1102)
- IP Teardrop (1103)
- ICMP Requests—Shows the packet count for the following signatures:
 - Echo Request (2004)
 - Time Request (2007)
 - Info Request (2009)
 - Address Mask Request (2011)
- ICMP Responses—Shows the packet count for the following signatures:
 - Echo Reply (2000)
 - Source Quench (2002)
 - Redirect (2003)
 - Time Exceeded (2005)
 - Parameter Problem (2006)
- ICMP Replies—Shows the packet count for the following signatures:
 - Unreachable (2001)
 - Time Reply (2008)
 - Info Reply (2010)
 - Address Mask reply (2012)
- ICMP Attacks—Shows the packet count for the following signatures:
 - Fragmented ICMP (2150)
 - Large ICMP (2151)
 - Ping of Death (2154)
- TCP Attacks—Shows the packet count for the following signatures:
 - No Flags (3040)
 - SYN & FIN Flags Only (3041)
 - FIN Flag Only (3042)
- UDP Attacks—Shows the packet count for the following signatures:
 - Bomb (4050)
 - Snork (4051)
 - Chargen (4052)
- DNS Attacks—Shows the packet count for the following signatures:
 - Host Info (6050)
 - Zone Transfer (6051)
 - Zone Transfer High Port (6052)
 - All Records (6053)
- FTP Attacks—Shows the packet count for the following signatures:
 - Improper Address (3153)
 - Improper Port (3154)

- RPC Requests to Target Hosts—Shows the packet count for the following signatures:
 - Port Registration (6100)
 - Port Unregistration (6101)
 - Dump (6102)
- YP Daemon Portmap Requests—Shows the packet count for the following signatures:
 - ypserv Portmap Request (6150)
 - yplib Portmap Request (6151)
 - yppasswdd Portmap Request (6152)
 - ypupdated Portmap Request (6153)
 - ypxfrd Portmap Request (6154)
- Miscellaneous Portmap Requests—Shows the packet count for the following signatures:
 - mountd Portmap Request (6155)
 - rexdb Portmap Request (6175)
- Miscellaneous RPC Calls—Shows the packet count for the following signatures:
 - rexdb Attempt (6180)
- RPC Attacks—Shows the packet count for the following signatures:
 - stadb Buffer Overflow (6190)
 - Proxied RPC (6103)
- Add—Click to add the selected graph type to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.
- Selected Graphs—Lists the graph types you want to show in the Selected Graphs list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

System Resources Graphs

This pane lets you view the status of the security appliance memory, CPU, and block utilization. This section includes the following topics:

- [Blocks](#)
- [CPU](#)
- [Memory](#)

Blocks

Blocks lets you view the free and used 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.

Fields

- Available Graphs —Lists the components you can graph.
 - Blocks Used—Displays the security appliance used memory blocks.
 - Blocks Free—Displays the security appliance free memory blocks.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. 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.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

CPU

This pane lets you view the CPU utilization. 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.

Fields

- Available Graphs—Lists the components you can graph.
 - CPU Utilization—Displays the security appliance CPU utilization.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. 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.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Memory

This pane lets you view the memory utilization. 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.

Fields

- Available Graphs—Lists the components you can graph.
 - Free Memory—Displays the security appliance free memory.
 - Used Memory—Displays the security appliance used memory.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. 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.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

WCCP

The Web Cache Communication Protocol redirects IPv4 traffic flows to web caches in real-time. In ASDM, you can monitor packet redirection of an interface using WCCP. WCCP also provides load balancing, scaling, fault tolerance, and fail safe services. Load balancing is provided by hashing based on the destination IP address. The hash values are used to choose the egress interface for any traffic flow. This protocol also enables the security appliance and WCCP clients to form service groups to support a service. This section includes the following topics:

- [Service Groups](#)
- [Redirection](#)

Service Groups

This pane allows you to view and refresh the service group, the display mode, and the hash settings.

Fields

- Service Group—Choose the applicable service group from the drop-down list.
- Display Mode—Choose the display mode from the drop-down list.
- Destination IP Address—Specify the destination IP address.
- Source IP Address—Specify the source IP address.
- Destination Port—Specify the destination port number.
- Source Port—Specify the source port number.

Redirection

This pane allows you to view and refresh WCCP interface statistics in either a summary or detailed format.

Fields

- Show Summary—Choose this option to display statistics in a summary format.
- Show Details—Choose this option to display statistics in a detailed format.