3

Status

This chapter describes how to view the status of your security appliance. It includes the following sections:

To access the Status pages, click **Status** in the left hand navigation pane.

Device Status Dashboard

Use the Status > Dashboard page to view information about the security appliance and its current settings.

Status > Dashboard

Field	Description
System Information	
System Name	Unit name of the device.

Field	Description
Firmware (Primary/Secondary)	Firmware version that the security appliance is currently using (Primary), and the firmware version that was previously running (Secondary). By default, the security appliance boots with the primary firmware.
Bootloader Version	Bootloader version of the security appliance.
Serial Number	Serial number of the security appliance.
PID	Product Identifier (PID) of the security appliance, also known as product name, model name, and product number.
UDI	Unique Device Identifier (UDI) of the security appliance. UDI is Cisco's product identification standard for hardware products.
Resource Utilization To see complete details for resource utilization, click **details**.	
CPU Utilization	Current CPU usage.
CPU Utilization Over 1 Minute	Average CPU usage in last one minute.
Memory Utilization	Total memory usage after the security appliance boots.
System Up Time	Duration for which the security appliance has been running.
Current Time	The current date and system time.
Licenses Displays the status of the security license that is used to activate security services. To manage the security license, click **manage**.	
Syslog Summary Displays the summary of the system event logs. Syslog entries can be of different severity levels. To see complete logs, click **details**.	
Emergency	Total number of Emergency logs. Click the number link for complete details.

Field	Description
Alert	Total number of Alert logs. Click the number link for complete details.
Critical	Total number of Critical logs. Click the number link for complete details.
Error	Total number of Error logs. Click the number link for complete details.
Warning	Total number of Warning logs. Click the number link for complete details.
Notification	Total number of Notification logs. Click the number link for complete details.
Information	Total number of Information logs. Click the number link for complete details.
Debug	Total number of Debug logs. Click the number link for complete details.
Site-to-Site VPN	
Displays the total number of active site-to-site VPN tunnels. To see complete details, click **details**.	
Remote Access VPN	
SSL Users	Total number of active SSL VPN users. Click the **SSL Users** link for complete details.
IPsec Users	Total number of active IPsec VPN users. Click the **IPsec Users** link for complete details. This option is only available when the security appliance is acting as an IPsec VPN server.
Routing Mode	
Displays the routing mode (NAT or Routing) between WAN and LAN. By default, the NAT mode is enabled. To enable or disable the Routing mode, click **details**.	
Physical Ports	
Name	Name of the physical port.
Port Type	Type of the physical port, such as WAN, LAN, or DMZ.

Field	Description
Mode	Link status of the physical port.
WAN Mode Displays the WAN operation mode, such as Single - WAN1, Failover, or Load Balancing. To see complete details for WAN redundancy, click **details.**	
WAN Interface(s) To see complete details for all WAN ports, click **details.**	
Name	Name of the WAN port.
IP Address	IP address for the WAN port.
LAN Interfaces To see complete details for all VLANs, click **details.**	
Index	ID of the VLAN.
Name	Name of the VLAN.
DHCP Mode	DHCP mode of the VLAN.
IP Address	Subnet IP address of the VLAN.
DMZ Interface To see complete details for all DMZs, click **details.**	
Port	Configurable port that is set as the DMZ port.
Name	Name of the DMZ port.
IP Address	Subnet IP address of the DMZ port.
Wireless Interfaces (for ISA550W and ISA570W only) To see complete details for all SSIDs, click **details.**	
SSID Number	Number of the SSID.
SSID Name	Name of the SSID.
VLAN	VLANs to which the SSID is mapped.
Client List	Number of client stations that are connected to the SSID.

Network Status

Use the Network Status pages to view information for the various interfaces, the network usage reports, the WAN bandwidth reports, all ARP (Address Resolution Protocol) entries, and DHCP address assignment. Refer to the following topics:

- **Status Summary, page 88**
- **Traffic Statistics, page 91**
- **Usage Reports, page 92**
- **WAN Bandwidth Reports, page 94**
- **ARP Table, page 95**
- **DHCP Bindings, page 95**
- **STP Status, page 96**
- **CDP Neighbor, page 98**

Status Summary

Use the Status Summary page to view information for the various interfaces.

Status Summary

Field	Description
Ethernet	
Port	Number of the physical port.
Name	Name of the physical port.
Enable	Shows if the physical port is enabled or disabled.
Port Type	Type of the physical port, such as WAN, LAN, or DMZ.
Line Status	Shows if the physical port is connected or not.
Speed/Duplex	Duplex mode (speed and duplex setting) of the physical port.
Mode	Access mode of the physical port. A WAN or DMZ port is always set to Access mode and a LAN port can be set to Access or Trunk mode.

Field	Description
VLAN	VLANs to which the physical port is mapped.
PVID	The Port VLAN ID (PVID) to be used to forward or filter the untagged packets coming into the port. The PVID of a Trunk port is fixed to the DEFAULT VLAN (1).
WAN	
Name	Name of the WAN port.
WAN Type	Network addressing mode used to connect to the Internet for the WAN port.
Connection Time	Time that the WAN port is connected, in seconds.
Connection Status	Shows if the WAN port obtains an IP address successfully or not. If yes, the connection status shows "Connected."
WAN State	Shows if the WAN port is active or inactive for routing. If the WAN port is active for routing, the WAN state shows "Up." If the WAN port is inactive for routing, the WAN state shows "Down." **NOTE:** The state "Down" means that the network detection fails. Even though the WAN state is down due to network detection failure, the WAN services (like SSL VPN and Remote Administration) can still be connected except the IPsec VPN Access service.
MAC Address	MAC address of the WAN port.
IP Address	IP address of the WAN port that is accessible from the Internet.
Subnet Mask/Prefix Length	Subnet mask or IPv6 prefix length for the WAN port.
Gateway	Default gateway for the WAN port.
DNS Server	DNS server for the WAN port.
Physical Port	Physical port that is associated with the WAN port.

Field	Description
Line Status	Shows if the cable is inserted to the WAN port or not. If the line status shows “Not Connected,” the cable may be loose or malfunctioning, or be plugged out. **NOTE:** If the line status shows “Not Connected,” the Connection Status will show “Not Connected” and the WAN State will show “Down.”
Zone	Zone to which the WAN port is assigned.
VLAN	
LAN MAC Address	MAC address of the default LAN.
Name	Name of the VLAN.
VID	ID of the VLAN.
IP Address	Subnet IP address of the VLAN.
Subnet Mask/Prefix Length	Subnet mask or IPv6 prefix length of the VLAN.
Physical Port	Physical ports that are assigned to the VLAN.
Zone	Zone to which the VLAN is mapped.
DMZ	
Physical Port	Physical port that is assigned to the DMZ.
Zone	Zone to which the DMZ is mapped.
Name	Name of the DMZ.
VID	ID of the VLAN.
IP Address	Subnet IP address of the DMZ.
Subnet Mask/Prefix Length	Subnet mask or IPv6 prefix length of the DMZ.

Traffic Statistics

Use the Traffic Statistics page to view traffic data for the various interfaces. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Click **Reset** to reset the values in the Ethernet table to zero.

Traffic Statistics

Field	Description
Ethernet	
Port	Name of the physical port.
Link Status	Shows if the port is connected or not.
Tx Packets	Number of IP packets transmitted by the port.
Rx Packets	Number of IP packets received by the port.
Collisions	Number of signal collisions that have occurred on this port. A collision occurs when the port tries to send data at the same time as a port on the other router or computer that is connected to this port.
Tx Bytes/Sec	Number of bytes transmitted by the port per second.
Rx Bytes/Sec	Number of bytes received by the port per second.
Uptime	Time that the port has been active. The uptime is reset to zero when the security appliance or the port is restarted.
WAN	
Name	Name of the WAN port.
Tx Packets	Number of IP packets transmitted by the WAN port.
Rx Packets	Number of IP packets received by the WAN port.
Collisions	Number of signal collisions that have occurred on this WAN port.
Tx Bytes/Sec	Number of bytes transmitted by the WAN port per second.
Rx Bytes/Sec	Number of bytes received by the WAN port per second.

Field	Description
Uptime	Time that the WAN port has been active. The uptime is reset to zero when the security appliance or the WAN port is restarted.
VLAN	
Name	Name of the VLAN.
Tx Packets	Number of IP packets transmitted by the VLAN.
Rx Packets	Number of IP packets received by the VLAN.
Collisions	Number of signal collisions that have occurred on this VLAN.
Tx Bytes/Sec	Number of bytes transmitted by the VLAN per second.
Rx Bytes/Sec	Number of bytes received by the VLAN per second.
Uptime	Time that the LAN port has been active.
DMZ	
Name	Name of the DMZ.
Tx Packets	Number of IP packets transmitted by the DMZ.
Rx Packets	Number of IP packets received by the DMZ.
Collisions	Number of signal collisions that occurred on the DMZ.
Tx Bytes/Sec	Number of bytes transmitted by the DMZ per second.
Rx Bytes/Sec	Number of bytes received by the DMZ per second.
Uptime	Time that the DMZ port has been active.

Usage Reports

Use the Usage Reports page to view the top 25 websites that have been most frequently visited, the top 25 users of Internet bandwidth by IP address, and the top 25 services and applications that consume the most bandwidth.

STEP 1 In the **Data Collection** area, enter the following information:

- **Enable Bandwidth Usage Report by IP Address:** Check this box to enable the bandwidth usage report sorted by the top 25 IP addresses that consume the most bandwidth.
- **Enable Bandwidth Usage Report by Internet Service:** Check this box to enable the bandwidth usage report sorted by the top 25 services and applications that consume the most bandwidth.
- **Enable Website Visits Report:** Check this box to enable the website visits report sorted by the top 25 URLs that have been most frequently visited.

STEP 2 Click **Save** to save your settings.

STEP 3 In the **Statistics Report** area, choose the desired report from the **Type** drop-down list to view.

- **Bandwidth Usage by IP Address:** This report displays the IP address of the top 25 users who consume the most bandwidth and the sum of bytes received and transmitted per IP address.
- **Bandwidth Usage by Internet Service:** This report displays the following information for the top 25 services and applications that consume the most bandwidth:
  - **Application:** The name for an known service or application or the port number for an unknown service or application. For example, if SMTP (6, 25) is displayed, SMTP is the service name, 6 is the protocol number, and 25 is the port number of the service.
  - **Sessions:** The total number of sessions for the service or application.
  - **Total Bandwidth (TX/RX):** The total number of bytes received and transmitted by the service or application during the period.
  - **Average Bandwidth (TX/RX):** The average number of bytes received and transmitted per second.

  This report is helpful to determine whether the services and applications being used are appropriate for your organization. You can block the services and applications that are consuming a large portion of available bandwidth. For information on blocking the applications, see Configuring Application Control, page 309.
- **Website Visits:** This report displays the URLs of the top 25 websites that have been most frequently visited and the number of hits to each website.

This report only monitors the website visits through the HTTP port specified in the advanced settings of either Firewall Content Filtering or Web URL Filtering. You can block the websites if inappropriate websites appear in this report. For information on blocking the websites, see Configuring Content Filtering to Control Internet Access, page 281, or Configuring Web URL Filtering, page 327.

STEP 4 Click **Refresh** to update the data on the screen, or click **Reset** to reset the values to zero.

- **Statistics Start Time:** Displays the time that the report starts collecting the data.

  NOTE: When a report is enabled or disabled or if you click **Reset**, the sample period for the report is reset.

- **Last Refresh Time:** Displays the time of your last refresh operation.

WAN Bandwidth Reports

Use the WAN Bandwidth page to view the real-time WAN network bandwidth usage per hour in the past 24 hours. This page is automatically updated every 10 seconds.

STEP 1 To enable the WAN bandwidth reports, check the box next to **Collect and Display WAN Bandwidth Statistics**.

STEP 2 Click **Save** to save your settings.

STEP 3 In the **Primary WAN** tab, you can see the real-time network bandwidth usage per hour in the past 24 hours for the primary WAN port.

STEP 4 In the **Secondary WAN** tab, you can see the real-time network bandwidth usage per hour in the past 24 hours for the secondary WAN port if a secondary WAN port is configured.

STEP 5 Click **Refresh** to manually refresh the data.

STEP 6 Click **Reset** to reset the WAN bandwidth usage data for both the primary WAN and the secondary WAN ports.

ARP Table

Address Resolution Protocol (ARP) is a computer-networking protocol that determines a network host's Link Layer or hardware address when only the Internet Layer (IP) or Network Layer address is known.

Use the ARP Table page to view information for all ARP entries. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

ARP Table

Field	Description
IP Address	IP address of the device.
Flag	Flag type of the device.
MAC Address	MAC address of the device, which is associated with the IP address.
Device	Device interface type.

DHCP Bindings

Use the DHCP Bindings page to view information for DHCP address assignment. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

DHCP Bindings

Field	Description
IP Address	IP address assigned to the host or the remote device.
MAC Address	MAC address of the host or the remote device.
Lease Start Time	The lease starting time of the IP address.
Lease End Time	The lease ending time of the IP address.

STP Status

Use the STP Status page to view information about VLANs that have Spanning Tree Protocol (STP) enabled. STP is a Link Layer network protocol that ensures a loop-free topology for any bridged LAN. No information is displayed for VLANs without STP enabled.

At the top of the page, use the **Check the STP status in this VLAN** list to choose a VLAN.

STP Status > Global Status

Field	Description
Bridge ID	An unique ID for the other devices on the network to identify this device.
Root Bridge ID	The bridge ID of the root bridge.
Root Port	The Port ID of the root port. The root port is the port with the lowest path cost to the root bridge. The root bridge does not have a root port.
Root Path Cost	The cost of the shortest path from the security appliance to the root bridge. The value 0 indicates that this security appliance is the root bridge.

Interface Status Table

Field	Description
Interface	The interface name.

Field	Description
Port Role	The role assigned to this port ▪ Root port: The port with the lowest path cost to the root bridge. ▪ Designated port: The port with the lowest path cost on a LAN segment. The LAN segment will use the designated port to reach the root bridge. ▪ Blocked port: The port that is neither a root port nor a designated port.
Path Cost	The cost of the path to root bridge through this port.
Priority	Priority of the port.
Port State	The state of the port: ▪ Disabled: This port is disabled. It will not transmit or receive any traffic. ▪ Blocking: This port is enabled but blocked by STP. It will not transmit or receive any traffic. ▪ Listening: This port will receive and process STP bridge protocol data units (BPDUs), but will not forward any data traffic. ▪ Learning: This port will start to learn MAC addresses from the received packets. It will also receive and process STP BPDUs, but will not forward any data traffic. ▪ Forwarding: This port will forward data traffic, process BPDUs and learn MAC address.
Designated Bridge ID	The ID of the designated bridge of the LAN segment. The designated bridge is used by all the other devices on the LAN segment to reach the root bridge.
Designated Port ID	The ID of the designated port of the LAN segment. The designated port is the port used by all the other devices on the LAN segment to reach the root bridge.

Field	Description
Designated Cost	The path cost to the designated bridge of the LAN segment.

CDP Neighbor

Use the CDP Neighbors page to view status information about neighboring devices that were discovered by the Cisco Discovery Protocol (if enabled). This information may be useful for troubleshooting.

The information on this page is automatically refreshed at 15-second intervals. If CDP is disabled, a message appears at the top of the page and the list is empty. To enable CDP, see CDP Discovery, page 432.

Field	Description
Device ID	The host name of the neighboring device.
Local Port	The outgoing port that the security appliance is using for this connection.
Duration	The time interval (in seconds) that the security appliance will keep CDP information from a neighboring device.
Function	The neighbor's device type: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, or r - repeater.
Platform	The model number of the neighboring device.
Interface ID	The interface that the neighboring device is using for the connection.
IP Address	The IP address of the neighboring device.
Duplex	The duplex mode of the connection.
Voice VLAN	The Voice VLAN ID of the neighboring device.

Wireless Status (for ISA550W and ISA570W only)

Use the Wireless Status pages to view information about your wireless network. Refer to the following topics:

- **Wireless Status, page 99**
- **Client Status, page 100**

Wireless Status

Use the Wireless Status > Wireless Status page to view the cumulative total of relevant wireless statistics for all SSIDs. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

Wireless Status > Wireless Status

Field	Description
Wireless Status	
SSID Number	Number of the SSID.
SSID Name	Name of the SSID.
MAC Address	MAC address of the SSID.
VLAN	VLAN to which the SSID is mapped.
Client List	Number of client stations that are connected to the SSID.
Wireless Statistics	
Name	Name of the SSID.
Tx Packets	Number of transmitted packets on the SSID.
Rx Packets	Number of received packets on the SSID.
Collisions	Number of packet collisions reported to the SSID.
Tx Bytes/Sec	Number of transmitted bytes of information on the SSID.
Rx Bytes/Sec	Number of received bytes of information on the SSID.

Field	Description
Uptime	Time that the SSID has been active.

Client Status

Use the Wireless Status > Client Status page to view information for all client stations that are already connected to each SSID. The MAC address and IP address for all connected client stations for each SSID are displayed. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

NAT Status

Use the NAT Status page to view information for all NAT rules.

NAT Status

Field	Description
Original Source Address	Original source IP address in the packet.
Original Destination Address	Original destination IP address in the packet.
Source Port	Source interface that traffic comes from.
Destination Port	Destination interface that traffic goes to.
Translated Destination Address	IP address that the specified original destination address is translated to.
Translated Source Address	IP address that the specified original source address is translated to.
Translated Destination Port	Interface that the specified destination interface is translated to.
Translated Source Port	Interface that the specified source interface is translated to.

Field	Description
Tx Packets	Number of transmitted packets.
Rx Packets	Number of received packets.
Tx Bytes/Sec	Volume in bytes of transmitted traffic.
Rx Bytes/Sec	Volume in bytes of received traffic.

VPN Status

Use the VPN Status pages to view information for all VPN sessions. Refer to the following topics:

- IPsec VPN Status, page 101
- SSL VPN Status, page 103

IPsec VPN Status

Use the VPN Status > IPsec VPN Status page to view information for all IPsec VPN sessions. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

VPN Status > IPsec VPN Status

Field	Description
Active Sessions To manually terminate an active IPsec VPN session, click the **Disconnect** icon in the **Connect** column. To manually terminate multiple active IPsec VPN sessions, check them and click the **Disconnect** button. If an IPsec VPN session is terminated, you can manually establish the VPN connection by clicking the **Connect** icon in the **Connect** column.	
Name	VPN policy used for an IPsec VPN session.
Status	Connection status for an IPsec VPN session.

Field	Description
VPN Type	VPN connection type for an IPsec VPN session, such as Site-to-Site, IPsec Remote Access, or Teleworker VPN Client.
WAN Interface	WAN port used for an IPsec VPN session.
Remote Gateway	IP address of the remote peer. **NOTE:** For a site-to-site VPN session, it displays the IP address of the remote gateway. For an IPsec VPN session between the Teleworker VPN client and a remote IPsec VPN server, it displays the IP address of the IPsec VPN server. For an IPsec VPN session between the IPsec VPN server and a remote VPN client, it displays the IP address of the remote VPN client.
Local Network	Subnet IP address and netmask of your local network.
Remote Network	Subnet IP address and netmask of the remote network.
Statistics	
Name	VPN policy used for an IPsec VPN session.
VPN Type	VPN connection type for an IPsec VPN session.
WAN Interface	WAN port used for an IPsec VPN session.
Remote Gateway	IP address of the remote peer.
Local Network	Subnet IP address and netmask of your local network.
Remote Network	Subnet IP address and netmask of the remote network.
Tx Bytes	Volume of traffic in kilobytes transmitted from the VPN tunnel.
Rx Bytes	Volume of traffic in kilobytes received from the VPN tunnel.
Tx Packets	Number of IP packets transmitted from the VPN tunnel.
Rx Packets	Number of IP packets received from the VPN tunnel.

Field	Description
Teleworker VPN Client If the Teleworker VPN Client feature is enabled and the security appliance is acting as a Cisco VPN hardware client, the following information is displayed.	
Status	Shows if the Teleworker VPN Client feature is enabled or disabled.
Primary DNS	IP address of the primary DNS server.
Secondary DNS	IP address of the secondary DNS server.
Primary WINS	IP address of the primary WINS server.
Secondary WINS	IP address of the secondary WINS server.
Default Domain	Default domain name.
Split Tunnel	IP address and netmask for the specified split subnets.
Split DNS	IP address or domain name for the specified split DNS.
Backup Server 1/2/3	IP address or hostname for the specified backup servers.

SSL VPN Status

Use the VPN Status > SSL VPN Status page to view information for all active SSL VPN sessions. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

VPN Status > SSL VPN Status

Field	Description
Active Sessions To manually terminate an active SSL VPN session, click the **Disconnect** icon in the **Configure** column. To manually terminate multiple active SSL VPN sessions, check them and click the **Disconnect** button.	
Session ID	ID of the SSL VPN session.

Field	Description
User Name	Name of the connected SSL VPN user.
Client IP (Actual)	Actual IP address used by the SSL VPN client.
Client IP (VPN)	Virtual IP address of the SSL VPN client assigned by the SSL VPN gateway.
Connect Time	Amount of time since the SSL VPN user first established the connection.

SSL VPN Statistics

In the **Global Status** area, the global statistic information is displayed. To clear the global statistic information, click **Clear**.

Active Users	Total number of connected SSL VPN users.
In CSTP Frames	Number of CSTP frames received from all clients.
In CSTP Bytes	Total number of bytes in the CSTP frames received from all clients.
In CSTP Data	Number of CSTP data frames received from all clients.
In CSTP Control	Number of CSTP control frames received from all clients.
Out CSTP Frames	Number of CSTP frames sent to all clients.
Out CSTP Bytes	Total number of bytes in the CSTP frames sent to all clients.
Out CSTP Data	Number of CSTP data frames sent to all clients.
Out CSTP Control	Number of CSTP control frames sent to all clients.

In the **Session Statistics** table, the following information for each SSL VPN session is displayed.

To clear the statistic information for a single SSL VPN session, click **Clear** in the **Configure** column. To clear the statistic information for multiple SSL VPN sessions, check them and click **-Clear**.

Session ID	ID of the SSL VPN session.
In CSTP Frames	Number of CSTP frames received from the client.

Field	Description
In CSTP Bytes	Total number of bytes in the CSTP frames received from the client.
In CSTP Data	Number of CSTP data frames received from the client.
In CSTP Control	Number of CSTP control frames received from the client.
Out CSTP Frames	Number of CSTP frames sent to the client.
Out CSTP Bytes	Total number of bytes in the CSTP frames sent to the client.
Out CSTP Data	Number of CSTP data frames sent to the client.
Out CSTP Control	Number of CSTP control frames sent to the client.

NOTE CSTP is a Cisco proprietary protocol for SSL VPN tunneling. "In" represents that the packet comes from the client. "Out" represents that the packet is sent to the client. The client is the PC running the Cisco AnyConnect Secure Mobility Client software that connects to the security appliance running the SSL VPN server. A CSTP frame is a packet that carrying CSTP protocol information. There are two major frame types, control frames and data frames. Control frames implement control functions within the protocol. Data frames carry the client data, such as the tunneled payload.

Active User Sessions

Use the Active User Sessions page to view information for all active user sessions that are currently logged into the security appliance. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Click the **Logout** icon to terminate a web login user session or a VPN user session.

Active User Sessions

Field	Description
User Name	Name of the logged user.
IP Address	Host IP address from which the user accessed the security appliance.

Field	Description
Login Method	How the user logs into the security appliance, such as WEB, SSL VPN, IPsec Remote Access, or Captive Portal.
Session Time	Time that the user has logged into the security appliance.

Security Services Reports

Use the Security Services Reports pages to view the reports for all security services. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Refer to the following topics:

- **Web Security Report, page 106**
- **Anti-Virus Report, page 107**
- **Email Security Report, page 108**
- **Network Reputation Report, page 109**
- **IPS Report, page 110**
- **Application Control Report, page 111**

NOTE The security services reports are only active when the security license is validated. Before you choose a security service report to view, make sure that the corresponding security service is enabled.

Web Security Report

This report displays the number of web access requests logged and the number of websites blocked by Web URL Filtering, Web Reputation Filtering, or both.

STEP 1 In the **Web Security** tab, specify the following information:

- **Enable:** Check this box to enable the web security report, or uncheck this box to disable it.

- **Blocked Requests:** Check this box to display the number of websites blocked by Web URL Filtering and/or Web Reputation Filtering in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and the time, the IP address and the MAC address of the host that initiated the request, the web site, the blocked URL, the filter that blocked the request, and the number of times that the connection was blocked.
- **Processed Requests:** Check this box to display the number of web access requests logged by Web URL Filtering and/or Web Reputation Filtering in the graph.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of web access requests processed and total number of websites blocked since the Web URL Filtering and Web Reputation Filtering services were activated.
Total Last 7 Days	Total number of web access requests processed and total number of websites blocked in last seven days.
Total Today	Total number of web access requests processed and total number of websites blocked in one day.
Graph	Total number of web access requests processed and total number of websites blocked per day in last seven days.

Anti-Virus Report

This report displays the number of files checked and the number of viruses detected by the Anti-Virus service.

STEP 1 In the **Anti-Virus** tab, specify the following information:

- **Enable:** Check this box to enable the Anti-Virus report, or uncheck this box to disable it.

- **Detected Requests:** Check this box to display the number of viruses detected by the Anti-Virus service in the graph. To view more information about detected requests, click the red bar in the graph. A pop-up window displays the following information for each detected request: the date and the time, the IP address and the MAC address of the source and of the destination, the protocol used for the connection, the action taken, and the number of times a virus was found.
- **Processed Requests:** Check this box to display the number of files checked by the Anti-Virus service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of files checked and total number of viruses detected since the Anti-Virus service was activated.
Total Last 7 Days	Total number of files checked and total number of viruses detected in last seven days.
Total Today	Total number of files checked and total number of viruses detected in one day.
Graph	Total number of files checked and total number of viruses detected per day in last seven days.

Email Security Report

This report displays the number of emails checked and the number of spam or suspected spam emails detected by the Spam Filter service.

STEP 1 In the **Email Security** tab, specify the following information:

- **Enable:** Check this box to enable the email security report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of spam or suspected spam emails detected by the Spam Filter service in the graph.

- **Processed Requests:** Check this box to display the number of emails checked by the Spam Filter service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of emails checked and total number of spam or suspected spam emails detected since the Spam Filter service was activated.
Total Last 7 Days	Total number of emails checked and total number of spam or suspected spam emails detected in last seven days.
Total Today	Total number of emails checked and total number of spam or suspected spam emails detected in one day.
Graph	Total number of emails checked and total number of spam or suspected spam emails detected per day in last seven days.

Network Reputation Report

This report displays the number of packets checked and the number of packets blocked by the Network Reputation service.

STEP 1 In the **Network Reputation** tab, specify the following information:

- **Enable:** Check this box to enable the network reputation report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets blocked by the Network Reputation service in the graph.
- **Processed Requests:** Check this box to display the number of packets checked by the Network Reputation service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets checked and total number of packets blocked since the Network Reputation service was activated.
Total Last 7 Days	Total number of packets checked and total number of packets blocked in last seven days.
Total Today	Total number of packets checked and total number of packets blocked in one day.
Graph	Total number of packets checked and total number of packets blocked per day in last seven days.

IPS Report

This report displays the number of packets detected and the number of packets dropped by the Intrusion Prevention (IPS) service.

STEP 1 In the **IPS** tab, specify the following information:

- **Enable:** Check this box to enable the IPS report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets dropped by the IPS service in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and time, the IP address and the MAC address of the source and of the destination, the action taken, and the number of times that this event was detected.
- **Processed Requests:** Check this box to display the number of packets detected by the IPS service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets detected and total number of packets dropped since the IPS service was activated.
Total Last 7 Days	Total number of packets detected and total number of packets dropped in last seven days.
Total Today	Total number of packets detected and total number of packets dropped in one day.
Graph	Total number of packets detected and total number of packets dropped per day in last seven days.

Application Control Report

This report displays the number of packets detected and the number of packets blocked by the Application Control service.

STEP 1 In the **Application Control** tab, specify the following information:

- **Enable:** Check this box to enable the application control report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets dropped by the Application Control service in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and time, the IP address and the MAC address of the host that initiated the request, the blocked application, and the number of times that the application was blocked.
- **Processed Requests:** Check this box to display the number of packets detected by the Application Control service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets detected and total number of packets blocked since the Application Control service was activated.
Total Last 7 Days	Total number of packets detected and total number of packets blocked in last seven days.
Total Today	Total number of packets detected and total number of packets blocked in one day.
Graph	Total number of packets detected and total number of packets blocked per day in last seven days.

System Status

Use the System Status pages to view information for all running processes and the system's CPU and memory utilization. Refer to the following topics:

- **Processes, page 112**
- **Resource Utilization, page 113**

Processes

Use the System Status > Processes page to view information for all running processes. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

System Status > Processes

Field	Description
Name	Name of the process that is running on your security appliance.
Description	Brief description for the running process.

Field	Description
Protocol	Protocol that is used by the socket.
Port	Port number of the local end of the socket.
Local Address	IP address of the local end of the socket.
Foreign Address	IP address of the remote end of the socket.

Resource Utilization

Use the System Status > Resource Utilization page to view information for the system's CPU and memory utilization.

System Status > Resource Utilization

Field	Description
CPU Utilization	
CPU Usage by User	CPU resource currently used by user space processes, in percentage.
CPU Usage by Kernel	CPU resource currently used by kernel space processes, in percentage.
CPU Idle	CPU idle resource at current time, in percentage.
CPU Waiting for I/O	CPU resource currently waiting for I/O, in percentage.
Memory Utilization	
Total Memory	Total amount of memory space available on the security appliance.
Memory Used	Total amount of memory space currently used by the processes.
Free Memory	Total amount of memory space currently not used by the processes.
Cached Memory	Total amount of memory space currently used as cache.

Field	Description
Buffer Memory	Total amount of memory space currently used as buffers.