



CHAPTER 42

Monitoring VPN

The VPN Monitoring sections show parameters and statistics for the following:

- VPN statistics for specific Remote Access, LAN-to-LAN, Clientless SSL VPN, and E-mail Proxy sessions
- Encryption statistics for tunnel groups
- Protocol statistics for tunnel groups
- Global IPSec and IKE statistics
- Crypto statistics for IPSec, IKE, SSL, and other protocols
- Statistics for cluster VPN server loads

VPN Connection Graphs

Displays VPN connection data in graphical or tabular form for the security appliance.

IPSec Tunnels

Use this window to specify graphs and tables of the IPSec tunnel types you want to view, or prepare to export or print.

Fields

- **Graph Window Title**—Displays the default title that appears in the window when you click Show Graphs. This attribute is particularly useful when you want to clarify data in that window before printing or exporting it. To change the title, select an alternative from the drop-down list or type the title.
- **Available Graphs**—Shows the types of active tunnels you can view. For each type you want to view collectively in a single window, click the entry in this box and click Add.
- **Selected Graphs**—Shows the types of tunnels selected.

If you click Show Graphs, ASDM shows the active tunnels types listed in this box in a single window.

A highlighted entry indicates the type of tunnel to be removed from the list if you click Remove.

- **Add**—Moves the selected tunnel type from the Available Graphs box to the Selected Graphs box.

- **Remove**—Moves the selected tunnel type from the Selected Graphs box to the Available Graphs box.
- **Show Graphs**—Displays a window consisting of graphs of the tunnel types displayed in the Selected Graphs box. Each type in the window displayed has a Graph tab and a Table tab you can click to alternate the representation of active tunnel data.

Modes

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

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

Sessions

Use this panel to specify graphs and tables of the VPN session types you want to view, or prepare to export or print.

Fields

- **Graph Window Title**—Displays the default title that appears in the window when you click Show Graphs. This attribute is particularly useful when you want to clarify data in that window before printing or exporting it. To change the title, select an alternative from the drop-down list or type the title.
- **Available Graphs**—Shows the types of active sessions you can view. For each type you want to view collectively in a single window, click the entry in this box and click Add.
- **Selected Graphs**—Shows the types of active sessions selected.

If you click Show Graphs, ASDM shows all of the active session types listed in this box in a single window.

A highlighted entry indicates the type of session to be removed from the list if you click Remove.

- **Add**—Moves the selected session type from the Available Graphs box to the Selected Graphs box.
- **Remove**—Moves the selected session type from the Selected Graphs box to the Available Graphs box.
- **Show Graphs**—Displays a window consisting of graphs of the session types displayed in the Selected Graphs box. Each type in the window displayed has a Graph tab and a Table tab you can click to alternate the representation of active session data.

Modes

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

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

VPN Statistics

These panels show detailed parameters and statistics for a specific remote-access, LAN-to-LAN, Clientless SSL VPN, or E-mail Proxy session. The parameters and statistics differ depending on the session protocol. The contents of the statistical tables depend on the type of connection you select. The detail tables show all the relevant parameters for each session.

Sessions

Use this panel to view session statistics for this server.

Fields

- Session types (unlabeled)—Lists the number of currently active sessions of each type, the total limit, and the total cumulative session count.
 - Remote Access—Shows the number of remote access sessions.
 - Site-to-Site—Shows the number of LAN-to-LAN sessions.
 - SSL VPN–Clientless—Shows the number of clientless browser-based VPN sessions.
 - SSL VPN–With Client—Shows the number of SSL VPN sessions requiring a client application on the remote computer.
 - SSL VPN–Total—Shows the number of client-based and clientless SSL VPN sessions.
 - E-mail Proxy—Shows the number of E-mail proxy sessions.
 - VPN Load Balancing—Shows the number of load-balanced VPN sessions
 - Total—Shows the total number of active concurrent sessions.
 - Total Cumulative—Shows the cumulative number of sessions since the last time the security appliance was rebooted or reset.
- Filter By—Specifies the type of sessions that the statistics in the following table represent.
 - Session type (unlabeled)—Designates the session type that you want to monitor. The default is Remote Access.
 - Session filter (unlabeled)—Designates which of the column heads in the following table to filter on. The default is --All Sessions--.
 - Filter name (unlabeled)—Specifies the name of the filter to apply. If you specify --All Sessions-- as the session filter list, this field is not available. For all other session filter selections, this field cannot be blank.
 - Filter—Executes the filtering operation.

The contents of the second table, also unlabeled, on this panel depend on the selection in the Filter By list. In the following list, the first-level bullets show the Filter By selection, and the second-level bullets show the column headings for this table.

- Remote Access—Indicates that the values in this table relate to remote access traffic.
 - Username/Tunnel Group—Shows the username or login name and the tunnel group for the session. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.
 - Assigned IP Address/Public IP Address—Shows the private (“assigned”) IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address, and it lets the client appear to be a host on the private network. Also shows the Public IP address of the client for this remote-access session. This is also known as the “outer” IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.
 - Protocol/Encryption—Shows the protocol and the data encryption algorithm this session is using, if any.
 - Login Time/Duration—Shows the date and time (MMM DD HH:MM:SS) that the session logged in. and the length of the session. Time is displayed in 24-hour notation.
 - Client Type/Version—Shows the type and software version number (for example, rel. 7.0_int 50) for connected clients, sorted by username.
 - Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the security appliance.
 - NAC Result and Posture Token—Displays values in this column only if you configured Network Admission Control on the security appliance.

The NAC Result shows one of the following values:

Accepted—ACS successfully validated the posture of the remote host.

Rejected—ACS could not successfully validate the posture of the remote host.

Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the security appliance.

Non-Responsive—The remote host did not respond to the EAPoUDP Hello message.

Hold-off—The security appliance lost EAPoUDP communication with the remote host after successful posture validation.

N/A—NAC is disabled for the remote host according to the VPN NAC group policy.

Unknown—Posture validation is in progress.

The posture token is an informational text string that is configurable on the Access Control Server. ACS downloads the posture token to the security appliance for informational purposes to aid in system monitoring, reporting, debugging, and logging. The typical value of the Posture Token field that follows the NAC Result field is as follows: Healthy, Checkup, Quarantine, Infected, or Unknown.

- Site-toSite—Indicates that the values in this table relate to LAN-to-LAN traffic.
 - Tunnel Group/IP Address—Shows the name of the tunnel group and the IP address of the peer.
 - Protocol/Encryption—Shows the protocol and the data encryption algorithm this session is using, if any.
 - Login Time/Duration—Shows the date and time (MMM DD HH:MM:SS) that the session logged in. and the length of the session. Time is displayed in 24-hour notation.

- Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the security appliance.
- Clientless SSL VPN—Indicates that the values in this table relate to Clientless SSL VPN traffic.
 - Username/IP Address—Shows the username or login name for the session and the IP address of the client.
 - Protocol/Encryption—Shows the protocol and the data encryption algorithm this session is using, if any.
 - Login Time/Duration—Shows the date and time (MMM DD HH:MM:SS) that the session logged in. and the length of the session. Time is displayed in 24-hour notation.
 - Client Type/Version—Shows the type and software version number (for example, rel. 7.0_int 50) for connected clients, sorted by username.
 - Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the security appliance.
- E-Mail Proxy—Indicates that the values in this table relate to traffic for Clientless SSL VPN sessions.
 - Username/IP Address—Shows the username or login name for the session and the IP address of the client.
 - Protocol/Encryption—Shows the protocol and the data encryption algorithm this session is using, if any.
 - Login Time/Duration—Shows the date and time (MMM DD HH:MM:SS) that the session logged in. and the length of the session. Time is displayed in 24-hour notation.
 - Client Type/Version—Shows the type and software version number (for example, rel. 7.0_int 50) for connected clients, sorted by username.
 - Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the security appliance.

The remainder of this section describes the buttons and fields beside and below the table.

- Details—Displays the details for the selected session. The parameters and values differ, depending on the type of session.
- Logout—Ends the selected session.
- Ping—Sends an ICMP ping (Packet Internet Groper) packet to test network connectivity. Specifically, the security appliance sends an ICMP Echo Request message to a selected host. If the host is reachable, it returns an Echo Reply message, and the security appliance displays a Success message with the name of the tested host, as well as the elapsed time between when the request was sent and the response received. If the system is unreachable for any reason, (for example: host down, ICMP not running on host, route not configured, intermediate router down, or network down or congested), the security appliance displays an Error screen with the name of the tested host.
- Logout By—Selects a criterion to use to filter the sessions to be logged out. If you select any but --All Sessions--, the box to the right of the Logout By list becomes active. If you selected the value Protocol for Logout By, the box becomes a list, from which you can select a protocol type to use as the logout filter. The default value of this list is IPsec. For all choices other than Protocol, you must supply an appropriate value in this box.
- Logout Sessions—Ends all sessions that meet the specified Logout By criteria.
- Refresh—Updates the screen and its data. The date and time indicate when the screen was last updated.

Modes

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

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

Sessions Details

The Session Details window displays configuration settings, statistics, and state information about the selected session.

The Remote Detailed table at the top of the Session Details window displays the following columns:

- Username—Shows the username or login name associated with the session. If the remote peer is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.
- Group Policy and Tunnel Group—Group policy assigned to the session and the name of the tunnel group upon which the session is established.
- Assigned IP Address and Public IP Address—Private IP address assigned to the remote peer for this session. Also called the inner or virtual IP address, the assigned IP address lets the remote peer appear to be on the private network. The second field shows the public IP address of the remote computer for this session. Also called the outer IP address, the public IP address is typically assigned to the remote computer by the ISP. It lets the remote computer function as a host on the public network.
- Protocol/Encryption—Protocol and the data encryption algorithm this session is using, if any.
- Login Time and Duration—Time and date of the session initialization, and the length of the session. The session initialization time is in 24-hour notation.
- Client Type and Version—Type and software version number (for example, rel. 7.0_int 50) of the client on the remote computer.
- Bytes Tx and Bytes Rx—Shows the total number of bytes transmitted to and received from the remote peer by the security appliance.
- NAC Result and Posture Token—The ASDM displays values in this column only if you configured Network Admission Control on the security appliance.

The NAC Result shows one of the following values:

- Accepted—The ACS successfully validated the posture of the remote host.
- Rejected—The ACS could not successfully validate the posture of the remote host.
- Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the security appliance.
- Non-Responsive—The remote host did not respond to the EAPoUDP Hello message.
- Hold-off—The security appliance lost EAPoUDP communication with the remote host after successful posture validation.
- N/A—NAC is disabled for the remote host according to the VPN NAC group policy.

- Unknown—Posture validation is in progress.

The posture token is an informational text string which is configurable on the Access Control Server. The ACS downloads the posture token to the security appliance for informational purposes to aid in system monitoring, reporting, debugging, and logging. The typical posture token that follows the NAC result is as follows: Healthy, Checkup, Quarantine, Infected, or Unknown.

The Details tab in the Session Details window displays the following columns:

- ID—Unique ID dynamically assigned to the session. The ID serves as the security appliance index to the session. It uses this index to maintain and display information about the session.
- Type—Type of session: IKE, IPSec, or NAC.
- Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol, and Port—Addresses and ports assigned to both the actual (Local) peer and those assigned to this peer for the purpose of external routing.
- Encryption—Data encryption algorithm this session is using, if any.
- Assigned IP Address and Public IP Address—Shows the private IP address assigned to the remote peer for this session. Also called the inner or virtual IP address, the assigned IP address lets the remote peer appear to be on the private network. The second field shows the public IP address of the remote computer for this session. Also called the outer IP address, the public IP address is typically assigned to the remote computer by the ISP. It lets the remote computer function as a host on the public network.
- Other—Miscellaneous attributes associated with the session.

The following attributes apply to an IKE session:

The following attributes apply to an IPSec session:

The following attributes apply to a NAC session:

- Revalidation Time Interval—Interval in seconds required between each successful posture validation.
- Time Until Next Revalidation—0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
- Status Query Time Interval—Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the security appliance to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
- EAPoUDP Session Age—Number of seconds since the last successful posture validation.
- Hold-Off Time Remaining—0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
- Posture Token—Informational text string configurable on the Access Control Server. The ACS downloads the posture token to the security appliance for informational purposes to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown.
- Redirect URL—Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the security appliance. The Redirect URL is an optional part of the access policy payload. The security appliance redirects all HTTP (port 80) and HTTPS (port 443) requests for the remote host to the Redirect URL if it is present. If the access policy does not contain a Redirect URL, the security appliance does not redirect HTTP and HTTPS requests from the remote host.

Redirect URLs remain in force until either the IPSec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.

More—Press this button to revalidate or initialize the session or tunnel group.

The ACL tab displays the ACL containing the ACEs that matched the session.

Modes

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

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

Sub-session Details – NAC Details

The NAC Details window lets you view the statistics and state of a NAC session, and revalidate and initialize the session or tunnel group.

The statistics and state attributes in this window are as follows:

- Reval Int (T)—Revalidation Time Interval. Interval in seconds required between each successful posture validation.
- Reval Left (T)—Time Until Next Revalidation. 0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
- SQ Int (T)—Status Query Time Interval. Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the security appliance to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
- EoU Age (T)—EAPoUDP Session Age. Number of seconds since the last successful posture validation.
- Hold Left (T)—Hold-Off Time Remaining. 0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
- Posture Token—Informational text string configurable on the Access Control Server. The ACS downloads the posture token to the security appliance for informational purposes to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown.
- Redirect URL—Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the security appliance. The Redirect URL is an optional part of the access policy payload. The security appliance redirects all HTTP (port 80) and HTTPS (port 443) requests for the remote host to the Redirect URL if it is present. If the access policy does not contain a Redirect URL, the security appliance does not redirect HTTP and HTTPS requests from the remote host.

Redirect URLs remain in force until either the IPSec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.

The buttons in this window are as follows:



Note

Choose **Monitoring > VPN > VPN Statistics > NAC Session Summary** if you want to revalidate or initialize all sessions that are subject to posture validation.

- **Revalidate Session**—Click if the posture of the peer or the assigned access policy (that is, the downloaded ACL, if any) has changed. Clicking this button initiates a new, unconditional posture validation. The posture validation and assigned access policy that were in effect before you clicked this button remain in effect until the new posture validation succeeds or fails. Clicking this button does not affect the session if it is exempt from posture validation.
- **Initialize Session**—Click if the posture of the peer or the assigned access policy (that is, the downloaded ACL, if any) has changed, and you want to clear the resources assigned to the session. Clicking the button purges the EAPoUDP association and access policy, and initiates a new, unconditional posture validation. The NAC default ACL is effective during the revalidation, so the session initialization can disrupt user traffic. Clicking this button does not affect the session if it is exempt from posture validation.
- **Revalidate Tunnel Group**—Click if the posture of the peers in the tunnel group occupied by the selected session or the assigned access policies (that is, the downloaded ACLs), have changed. Clicking this button initiates new, unconditional posture validations. The posture validation and assigned access policy that were in effect for each session in the tunnel group before you clicked this button remain in effect until the new posture validation succeeds or fails. Clicking this button does not affect sessions that are exempt from posture validation.
- **Initialize Tunnel Group**—Click if the posture of the peers in the tunnel group occupied by the selected session, or the assigned access policies (that is, the downloaded ACLs), have changed, and you want to clear the resources assigned to the sessions. Clicking this button purges the EAPoUDP associations and access policies (that is, the downloaded ACLs, if any) used for posture validation in the tunnel group occupied by the selected session, and initiates new, unconditional posture validations for the effected peers. The NAC default ACL is effective during the revalidations, so the session initializations can disrupt user traffic. Clicking this button does not affect sessions that are exempt from posture validation.

Modes

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

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

Encryption Statistics

This panel shows the data encryption algorithms used by currently active user and administrator sessions on the security appliance. Each row in the table represents one encryption algorithm type.

Fields

- **Show Statistics For**—Selects a specific server or group or all tunnel groups.

- Encryption Statistics—Shows the statistics for all the data encryption algorithms in use by currently active sessions.
 - Encryption Algorithm—Lists the encryption algorithm to which the statistics in this row apply.
 - Sessions—Lists the number of sessions using this algorithm.
 - Percentage—Indicates the percentage of sessions using this algorithm relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).
- Total Active Sessions—Shows the number of currently active sessions.
- Cumulative Sessions—Shows the total number of sessions since the security appliance was last booted or reset.
- Refresh—Updates the statistics shown in the Encryption Statistics table.

Modes

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

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

NAC Session Summary

Monitoring > VPN > VPN Statistics > NAC Session Summary

The NAC Session Summary window lets you view the active and cumulative Network Admission Control sessions.

Fields

- Active NAC Sessions—General statistics about remote peers that are subject to posture validation.
- Cumulative NAC Sessions—General statistics about remote peers that are or have been subject to posture validation.
- Accepted—Number of peers that passed posture validation and have been granted an access policy by an Access Control Server.
- Rejected—Number of peers that failed posture validation or were not granted an access policy by an Access Control Server.
- Exempted—Number of peers that are not subject to posture validation because they match an entry in the Posture Validation Exception list configured on the security appliance.
- Non-responsive—Number of peers not responsive to Extensible Authentication Protocol (EAP) over UDP requests for posture validation. Peers on which no CTA is running do not respond to these requests. If the security appliance configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the security appliance for these peers. Otherwise, the security appliance assigns the NAC default policy.
- Hold-off—Number of peers for which the security appliance lost EAPoUDP communications after a successful posture validation. The NAC Hold Timer attribute (Configuration > VPN > NAC) determines the delay between this type of event and the next posture validation attempt.

- N/A—Number of peers for which NAC is disabled according to the VPN NAC group policy.
- Revalidate All—Click if the posture of the peers or the assigned access policies (that is, the downloaded ACLs), have changed. Clicking this button initiates new, unconditional posture validations of all NAC sessions managed by the security appliance. The posture validation and assigned access policy that were in effect for each session before you clicked this button remain in effect until the new posture validation succeeds or fails. Clicking this button does not affect sessions that are exempt from posture validation.
- Initialize All—Click if the posture of the peers or the assigned access policies (that is, the downloaded ACLs) have changed, and you want to clear the resources assigned to the sessions. Clicking this button purges the EAPoUDP associations and assigned access policies used for posture validations of all NAC sessions managed by the security appliance, and initiates new, unconditional posture validations. The NAC default ACL is effective during the revalidations, so the session initializations can disrupt user traffic. Clicking this button does not affect sessions that are exempt from posture validation.

Modes

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

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

Protocol Statistics

This panel displays the protocols used by currently active user and administrator sessions on the security appliance. Each row in the table represents one protocol type.

Fields

- Show Statistics For—Selects a specific server or group or all tunnel groups.
- Protocol Statistics—Shows the statistics for all the protocols in use by currently active sessions.
 - Protocol—Lists the protocol to which the statistics in this row apply.
 - Sessions—Lists the number of sessions using this protocol.
 - Percentage—Indicates the percentage of sessions using this protocol relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).
- Total Active Sessions—Shows the number of currently active sessions.
- Cumulative Sessions—Shows the total number of sessions since the security appliance was last booted or reset.
- Refresh—Updates the statistics shown in the Protocol Statistics table.

Modes

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

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

VLAN Mapping Sessions

This panel displays the number of sessions assigned to an egress VLAN, as determined by the value of the Restrict Access to VLAN parameter of each group policy in use. The security appliance forwards all traffic to the specified VLAN.

Field

- Active VLAN Mapping Sessions—Number of VPN sessions assigned to an egress VLAN.

Modes

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

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

Global IKE/IPSec Statistics

This panel displays the global IKE/IPSec statistics for currently active user and administrator sessions on the security appliance. Each row in the table represents one global statistic.

Fields

- Show Statistics For—Selects a specific protocol, IKE Protocol (the default) or IPSec Protocol.
- Global IKE/IPSec Statistics—Shows the statistics for all the protocols in use by currently active sessions.
 - Statistic—Lists the name of the statistical variable. The contents of this column vary, depending upon the value you select for the Show Statistics For parameter.
 - Value—The numerical value for the statistic in this row.
- Refresh—Updates the statistics shown in the Global IKE/IPSec Statistics table.

Modes

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

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

Crypto Statistics

This panel displays the crypto statistics for currently active user and administrator sessions on the security appliance. Each row in the table represents one crypto statistic.

Fields

- Show Statistics For—Selects a specific protocol, IKE Protocol (the default), IPSec Protocol, SSL Protocol, or other protocols.
- Crypto Statistics—Shows the statistics for all the protocols in use by currently active sessions.
 - Statistic—Lists the name of the statistical variable. The contents of this column vary, depending upon the value you select for the Show Statistics For parameter.
 - Value—The numerical value for the statistic in this row.
- Refresh—Updates the statistics shown in the Crypto Statistics table.

Modes

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

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

Compression Statistics

This panel displays the compression statistics for currently active user and administrator sessions on the security appliance. Each row in the table represents one compression statistic.

Fields

- Show Statistics For—Lets you select compression statistics for clientless SSL VPN or SSL VPN Client sessions.
- Statistics—Shows all the statistics for the selected VPN type.
 - Statistic—Lists the name of the statistical variable. The contents of this column vary, depending upon the value you select for the Show Statistics For parameter.
 - Value—The numerical value for the statistic in this row.
- Refresh—Updates the statistics shown in the Compression Statistics table.

Modes

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

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

Cluster Loads

Use this panel to view the current traffic load distribution among the servers in a VPN load-balancing cluster. If the server is not part of a cluster, you receive an information message saying that this server does not participate in a VPN load-balancing cluster.

Fields

- VPN Cluster Loads—Displays the current load distribution in the VPN load-balancing cluster. Clicking a column heading sorts the table, using the selected column as the sort key.
 - Public IP Address—Displays the externally visible IP address for the server.
 - Role—Indicates whether this server is a master or backup device in the cluster.
 - Priority—Shows the priority assigned to this server in the cluster. The priority must be an integer in the range of 1 (lowest) to 10 (highest). The priority is used in the master-election process as one way to determine which of the devices in a VPN load-balancing cluster becomes the master or primary device for the cluster.
 - Model—Indicates the security appliance model name and number for this server.
 - Load %—Indicates what percentage of a server's total capacity is in use, based upon the capacity of that server.
 - Sessions—Shows the number of currently active sessions.
- Refresh—Loads the table with updated statistics.

Modes

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

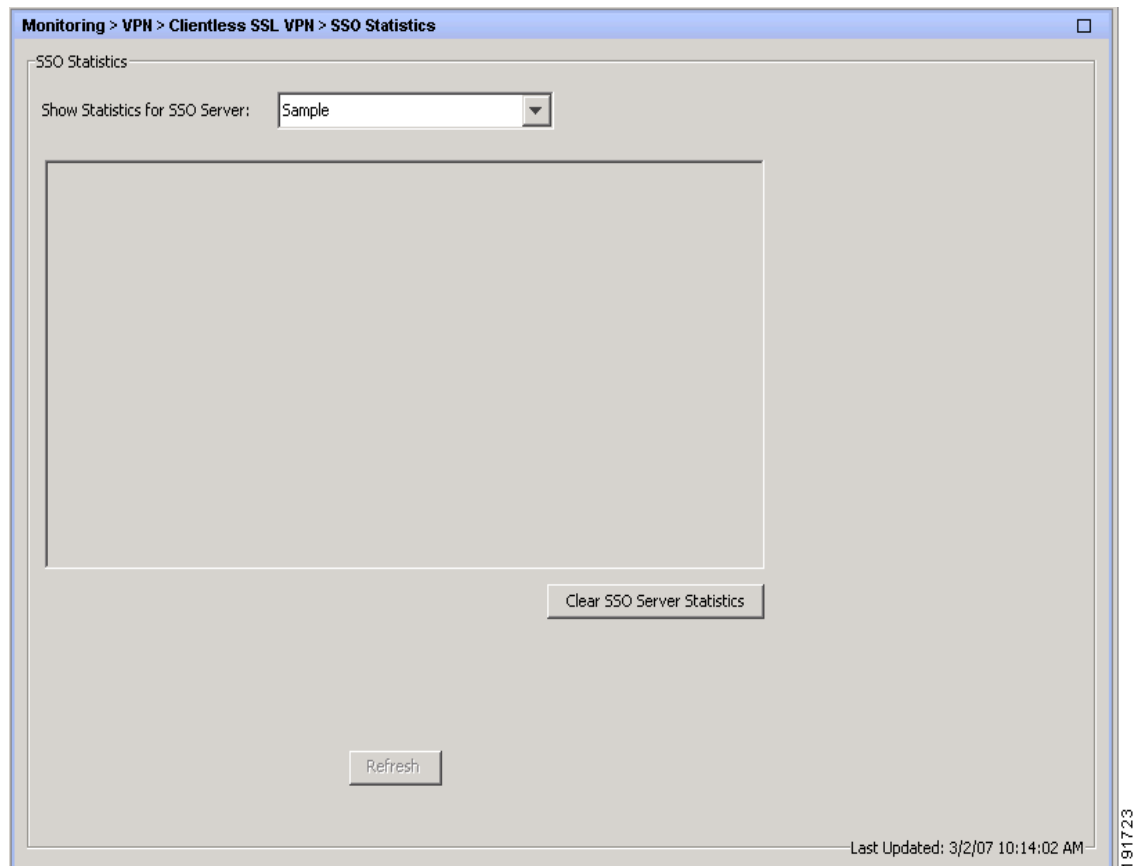
Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

SSO Statistics for Clientless SSL VPN Session

This panel displays the single sign-on statistics for currently active SSO servers configured for the security appliance.

**Note**

These statistics are for SSO with SiteMinder and SAML Browser Post Profile servers only.

**Fields**

- Show Statistics For SSO Server — Selects an SSO server.
- SSO Statistics—Shows the statistics for all the currently active sessions on the selected SSO server.

SSO statistics that display include:

- Name of SSO server
- Type of SSO server
- Authentication Scheme Version (SiteMinder servers)
- Web Agent URL (SiteMinder servers)
- Assertion Consumer URL (SAML POST servers)
- Issuer (SAML POST servers)
- Number of pending requests
- Number of authorization requests
- Number of retransmissions
- Number of accepts

- Number of rejects
- Number of timeouts
- Number of unrecognized responses
- Refresh—Updates the statistics shown in the SSO Statistics table
- Clear SSO Server Statistics—Resets statistics for the displayed server.

Modes

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

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