CHAPTER 31

Monitoring VPN

This chapter describes how to use VPN monitoring parameters and statistics for the following:

- VPN statistics for specific Remote Access and LAN-to-LAN 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 ASA 1000V.

IPsec Tunnels

Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels

Use this pane 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 pane when you click Show Graphs. This attribute is particularly useful when you want to clarify data in that pane before printing or exporting it. To change the title, choose 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 pane, choose the entry and click **Add**.
- Selected Graphs—Shows the types of tunnels selected.

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

  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 column to the Selected Graphs column.

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

Sessions

Monitoring > VPN > VPN Connection Graphs > Sessions

Use this pane 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 panepane when you click Show Graphs. This attribute is particularly useful when you want to clarify data in that pane 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 pane, 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 pane.

  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 pane consisting of graphs of the session types displayed in the Selected Graphs box. Each type in the pane displayed has a Graph tab and a Table tab you can click to alternate the representation of active session data.

VPN Statistics

These panes show detailed parameters and statistics for a specific remote-access and LAN-to-LAN sessions. The parameters and statistics differ depending on the session protocol. The contents of the statistical tables depend on the type of connection you choose. The detail tables show all the relevant parameters for each session.

Sessions

Monitoring > VPN > VPN Statistics > Sessions

Use this pane to view session statistics for the adaptive security appliance.

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 client-based SSL VPN sessions. With ASA version 8.x and above , this represents the AnyConnect SSL VPN client 2.x and above.
  - SSL VPN–Inactive—Shows the number of SSL VPN sessions that are inactive on the remote computer.

Note An administrator can keep track of the number of users in the inactive state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in. You can also access these statistics using the **show vpn-sessiondb** CLI command (refer to the *Cisco Security Appliance Command Reference Guide)*.

  - 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 ASA 1000V 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 IPsec 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, in this pane 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 (IPsec software and hardware clients) traffic.
  - Username/Connection Profile—Shows the username or login name and the connection profile (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.
  - Group Policy Connection Profile—Displays the tunnel group policy connection profile for the session.

  - 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.

Note The Assigned IP Address field does not apply to Clientless SSL VPN sessions, as the ASA (proxy) is the source of all traffic . For a hardward client session in Network Extension mode, the Assigned IP address is the subnet of the hardware client's private/inside network interface.

  - 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 (Peer) 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 ASA 1000V.
- IPsec Site-to-Site—Indicates that the values in this table relate to LAN-to-LAN traffic.
  - Connection Profile/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 ASA 1000V.
- 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.
  - Group Policy Connection Profile—Displays the connection profile of the tunnel group policy.
  - 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 ASA 1000V.
- SSL VPN Client—Indicates that the values in this table relate to traffic for SSL VPN Client sessions.
  - Username/IP Address—Shows the username or login name for the session and the IP address of the client.
  - Group Policy Connection Profile—Displays the connection profile of the tunnel group policy.
  - 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 ASA 1000V.
- 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.
  - Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the ASA 1000V.

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 ASA 1000V sends an ICMP Echo Request message to a selected host. If the host is reachable, it returns an Echo Reply message, and the ASA 1000V 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 ASA 1000V displays an Error screen with the name of the tested host.
- Logout By—Chooses a criterion to use to filter the sessions to be logged out. If you choose any but --All Sessions--, the box to the right of the Logout By list becomes active. If you choose the value Protocol for Logout By, the box becomes a list, from which you can choose 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 column.
- 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.

Sessions Details

Monitoring > VPN > VPN Statistics > Sessions >Details

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

The Remote Detailed table at the top of the Session Details pane 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 ASA 1000V.
- NAC Result and Posture Token—The ASDM displays values in this column only if you configured Network Admission Control on the ASA 1000V.

  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 ASA 1000V.
  - Non-Responsive—The remote host did not respond to the EAPoUDP Hello message.
  - Hold-off—The ASA 1000V 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 ASA 1000V 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 panepane displays the following columns:

- ID—Unique ID dynamically assigned to the session. The ID serves as the ASA 1000V 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 ASA 1000V 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 ASA 1000V 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 ASA 1000V. The Redirect URL is an optional part of the access policy payload. The ASA 1000V 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 ASA 1000V 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.

Crypto Statistics

Monitoring > VPN > VPN Statistics > Crypto Statistics

This pane displays the crypto statistics for currently active user and administrator sessions on the ASA 1000V. 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.
- 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.

Encryption Statistics

Monitoring > VPN > VPN Statistics > Encryption Statistics

This pane shows the data encryption algorithms used by currently active user and administrator sessions on the ASA 1000V. 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 ASA 1000V was last booted or reset.
- Refresh—Updates the statistics shown in the Encryption Statistics table.

Global IKE/IPsec Statistics

Monitoring > VPN > VPN Statistics > Global IKE/IPSec Statistics

This pane displays the global IKE/IPsec statistics for currently active user and administrator sessions on the ASA 1000V. Each row in the table represents one global statistic.

Fields

- Show Statistics For—Selects a specific protocol, IKE Protocol (the default) or IPsec Protocol.
- 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.

Protocol Statistics

Monitoring > VPN > VPN Statistics > Protocol Statistics

This pane displays the protocols used by currently active user and administrator sessions on the ASA 1000V. 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 Tunnel—Shows the number of currently active sessions.
- Cumulative Tunnels—Shows the total number of sessions since the ASA 1000V was last booted or reset.
- Refresh—Updates the statistics shown in the Protocol Statistics table.