

Monitor VPN

- Monitor VPN Connection Graphs, on page 1
- Monitor VPN Statistics, on page 1

Monitor VPN Connection Graphs

See the following screens for showing VPN connection data in graphical or tabular form for the ASA.

Monitor IPsec Tunnels

Monitoring> VPN> VPN Connection Graphs> IPSec Tunnels

For specifying graphs and tables of the IPsec tunnel types that you want to view or to prepare for export or print.

Monitor Sessions

Monitoring> VPN> VPN Connection Graphs> Sessions

For specifying graphs and table of the VPN session types that you want to view or to prepare for export or print.

Monitor VPN Statistics

See the following screens for showing detailed parameters and statistics for a specific remote-access or LAN-to-LAN session. 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.

Monitor Session Window

Monitoring> VPN> VPN Statistics> Sessions

For viewing VPN session statistics for the ASA. The contents of the second table in this pane depend on the selection in the Filter By list.

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 appropriate release of the Cisco ASA Command Reference Guide.

- All 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.
- Ping—Sends an ICMP ping (Packet Internet Groper) packet to test network connectivity. Specifically, the ASA sends an ICMP Echo Request message to a selected host. If the host is reachable, it returns an Echo Reply message, and the ASA 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 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.

Monitor Active VPN Sessions

Monitoring > VPN > VPN Statistics > Sessions

For viewing Secure Client sessions sorted by username, IP address, address type, or public address.

Monitor VPN Session Details

Monitoring> VPN> VPN Statistics> Sessions> Details

For viewing configuration settings, statistics, and state information about the selected session.

- NAC Result and Posture Token

The ASDM displays values in this column only if you configured Network Admission Control on the ASA.

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

- ID—Unique ID dynamically assigned to the session. The ID serves as the ASA 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 IKE sessions, IPsec sessions, and NAC sessions:

- 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 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 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. The Redirect URL is an optional part of the access policy payload. The ASA 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 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.

Monitor Cluster Loads

Monitoring> VPN> VPN Statistics> Cluster Loads

For viewing 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.

Monitor Crypto Statistics

Monitoring > VPN> VPN Statistics> Crypto Statistics

For viewing the crypto statistics for currently active user and administrator sessions on the ASA. Each row in the table represents one crypto statistic.

Monitor Compression Statistics

Monitoring> VPN> VPN Statistics> Compression Statistics

For viewing the compression statistics for currently active user and administrator sessions on the ASA. Each row in the table represents one compression statistic.

Monitor Encryption Statistics

Monitoring> VPN> VPN Statistics> Encryption Statistics

For viewing the data encryption algorithms used by currently active user and administrator sessions on the ASA. Each row in the table represents one encryption algorithm type.

Monitor Global IKE/IPsec Statistics

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

For viewing the global IKE/IPsec statistics for currently active user and administrator sessions on the ASA. Each row in the table represents one global statistic.

Monitor NAC Session Summary

For viewing the active and cumulative Network Admission Control sessions.

- 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 ASA.
- 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 ASA configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the ASA for these peers. Otherwise, the ASA assigns the NAC default policy.
- Hold-off—Number of peers for which the ASA 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 ASA. 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 ASA, 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.

Monitor Protocol Statistics

Monitoring> VPN> VPN Statistics> Protocol Statistics

For viewing the protocols used by currently active user and administrator sessions on the ASA. Each row in the table represents one protocol type.

Monitor VLAN Mapping Sessions

For viewing 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 ASA forwards all traffic to the specified VLAN.