CHAPTER 5

Monitoring Remote Access VPN Services

A remote access service (RAS) VPN secures connections for remote users, such as mobile users or telecommuters. RAS VPN monitoring provides all of the most important indicators of cluster, concentrator, and user session performance at a glance.

Performance Monitor also enables you to determine quickly whether RAS VPN problems exist and where they exist. You can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users.

Optionally, you can logout one RAS user at a time.

Tip To troubleshoot common problems with RAS VPN services, see the Troubleshooting appendix.

The following topics explain the RAS VPN monitoring features:

Understanding RAS Virtual Clusters

Note

- References in Performance Monitor and documentation to *load balancing services* pertain only to the web server load-balancing capabilities of content switching services modules. Performance Monitor does not monitor the load balancing of concentrators or appliances that you have combined in virtual clusters.
- Although PIX OS and Easy VPN both support the use of RAS VPNs, neither technology supports the use of virtual clusters.

RAS VPNs enable remote users to participate in private networks through a shared public infrastructure, connecting through dial-up, ISDN, DSL, cable, or other technologies.

Performance Monitor monitors RAS VPN services that originate on several different kinds of devices, but special considerations apply to Cisco VPN 3000 Series concentrators and ASA 5520 or 5550 appliances because you can monitor them singly or when they are combined in a *virtual cluster* for load-balancing. In a virtual cluster, a collection of concentrators or a collection of appliances can function as a single entity.

The cluster is known to the outside client space by one IP address. The virtual IP address must be a routable address—meaning a valid address to which another device can send packets. Otherwise, inbound packets do not reach the cluster.

This virtual IP address is not tied to a specific device in the VPN cluster. It is serviced by the *virtual cluster master*. A virtual cluster master concentrator maintains the load information from all secondary concentrators or appliances in a specific cluster. Each secondary concentrator sends KeepAlive load information messages to the master.

- The VPN 3000 series includes six different concentrator models. To learn about their uses and capabilities, which can help you to assess whether the concentrators that you monitor are operating correctly, see http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/index.html.
- To learn about ASA 5520 and 5550 appliance uses and capabilities, see http://www.cisco.com/en/US/products/ps6120/index.html.

Understanding Easy VPN

Cisco Easy VPN, a software enhancement for several kinds of Cisco devices, greatly simplifies VPN deployment for remote offices and teleworkers. Easy VPN centralizes VPN management across many devices, thus reducing the complexity of VPN deployments. Easy VPN implementations require that you use both a Cisco Easy VPN Server and the Cisco Easy VPN Remote feature in your supported devices.

Supported routers, appliances, firewalls, and concentrators act like remote VPN clients when you use Easy VPN. As such, these devices can receive security policies from an Easy VPN server, which minimizes the VPN configuration requirements at remote locations in your organization.

In addition, a device enabled with Cisco Easy VPN Server can terminate VPN tunnels initiated by mobile remote workers who run Cisco VPN client software on their PCs.

Performance Monitor represents all Easy VPN sessions as if they are RAS VPN sessions, even though an Easy VPN server allows supported routers, appliances, firewalls, and concentrators to act as VPN head-end devices in either site-to-site or remote-access VPNs.

To learn about Easy VPN, see: http://www.cisco.com/en/US/products/sw/secursw/ps5299/index.html.

Note

- Easy VPN does not support the use of RAS clusters.
- Performance Monitor does not display Easy VPN session usernames, and does not associate usernames with specific Easy VPN sessions.
- The User Session Report feature in Performance Monitor does not support Easy VPN.

Working in the RAS Clusters Table

Performance Monitor provides a high-level overview that shows all of your remote access clusters. Use this overview to isolate user data and concentrator data, and display subsets of available cluster statistics.

Tip Performance Monitor updates its record of cluster membership automatically once each day. If you add or delete VPN concentrators in a cluster or if you move a concentrator from one cluster to another, you must select **Devices > Importing Devices**, then click **Revalidate**. Otherwise, displayed information is wrong for the relevant cluster until the next automatic update.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Clusters**. For an explanation of the columns in the table, see Table 5-1.

Performance Monitor averages its measurements of VPN concentrator health and performance to arrive at the high-level statistics it displays for the clusters in your network.

Step 2 You can do any of the following to further refine the list or to obtain more detailed information:

- To find a device in the list, enter the IP address or DNS name of the device in the Find Device field and click **Find**. If the device can be found, the Remote Access Device Graphs page displays information about the specified concentrator. For information on the types of graphs, see Viewing Detail Graphs for a RAS Device, page 5-4.
- To display a graph of dropped packets for a RAS cluster, click the relevant entry in the Packet Drop % column.
- To display a throughput graph for a RAS cluster, click the relevant entry in the Throughput (kbps) column.
- To display a graph of bandwidth usage for a RAS cluster, click the relevant entry in the Bandwidth Usage % column.

Reference

Table 5-1 Remote Access Clusters Page

Element	Description
Cluster column	Displays the DNS name of the virtual cluster master.
Devices column	Displays the total number of devices in the cluster.
Master Device column	Displays the IP address of the master device on the specified cluster. The virtual cluster master concentrator maintains the load information from all secondary concentrators in the cluster. Each secondary sends load information in the KeepAlive message exchange to the master.
# of Users column	Displays the aggregate total number of active sessions on all RAS devices. **Note** If you or one of your colleagues log out a RAS user, this value might differ the next time the display is refreshed.
Load Variance column	Indicates skew, calculated by measuring the difference between the device with the highest load and the device with the lowest load. Device load is calculated as a percentage of current active sessions divided by the configured maximum-allowed connections.

Table 5-1 Remote Access Clusters Page (continued)

Element	Description
Packet Drop % column	Displays the computation of dropped packets in IPSec Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all inbound and outbound packets on all RAS devices. Click any hyperlinked entry in the Packets Drop column to open a new browser that displays your selection as a graph.
Throughput (kbps) column	Displays the sum of outbound and inbound octets across public interfaces on all RAS devices. Click any hyperlinked entry in the Throughput (kbps) column to open a new browser that displays your selection as a graph.
Bandwidth Usage % column	Displays an averaged percentage that shows bandwidth used by all RAS devices, divided by bandwidth available to all RAS devices. Click any hyperlinked entry in the Bandwidth Usage % column to open a new browser that displays your selection as a graph.
Inbound Connection Failure % column	Displays an averaged percentage that shows the inbound Phase-1 (IKE) and Phase-2 (IPSec) connections that were initiated remotely and failed, over all inbound connection attempts.

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Working with RAS Devices

See the following topics to learn how to isolate and monitor information that describes the status of any validated VPN concentrator:

- Viewing Detail Graphs for a RAS Device, page 5-4
- Monitoring RAS Device Usage and Activity, page 5-6
- Monitoring RAS Device Failures, page 5-7
- Monitoring RAS Device Crypto Activity, page 5-8
- Viewing RAS Device Crypto Accelerator Card Data, page 5-10
- Viewing the Remote Access Interfaces Table, page 5-10

Viewing Detail Graphs for a RAS Device

You can isolate information about a validated Cisco VPN 3000 Series concentrator in your network and display detailed graphs that describe its health and performance.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Device Details**.

By default, the Remote Access Device Graphs page displays graphs that describe the health and performance of whichever device uses the lowest number as its IP address. For a description of the graphs, see Table 5-2.

Note A known problem might interfere with your ability to interpret a graph that uses two vertical (Y) axes. The first Y axis always begins at zero, but the second Y axis begins at the lowest value for the specified time range—even when that value is greater than zero. Thus, the two Y axes might not be directly comparable.

Step 2 Select the device whose graphs you want to view from the **Select Device** list.

Types of RAS Graphs

Table 5-2 Types of RAS Graphs

Graph Type	Description
Bandwidth Utilization	Illustrates percentages of device bandwidth capacity used on the public interface: • The vertical axis shows the average percentage of bandwidth capacity used in a specific polling cycle. • The horizontal axis shows the time of day for the polling cycle.
CPU Usage	Illustrates used percentages of device CPU capacity: • The vertical axis shows the average percentage of CPU capacity used in a specific polling cycle. • The horizontal axis shows time of day for the polling cycle.
Inbound Connect Failures	Illustrates the trend of inbound connection failures over time: • The vertical axis shows the average number of failures in a specific polling cycle. • The horizontal axis shows time of day for the polling cycle.
Throughput vs. Session	Displays a line graph that helps you compare throughput trends to the trend of the number of VPN sessions over time: • Because it shows two kinds of information, it has two vertical axes: – The vertical axis on the left (orange) shows the average throughput in a specific polling cycle, in bytes. – The vertical axis on the right (blue) shows the average number of sessions in a specific polling cycle. • The horizontal axis shows the time of day at which Performance Monitor calculated the trends in each vertical axis.
IKE Phase 1 Connection Failures	Illustrates the percentage of failures in Phase-1 (IKE) connections: • The vertical axis shows the average percentage of failed connections in a specific polling cycle. • The horizontal axis shows time of day for the polling cycle.
IPSec Phase 2 Connection Failures	Illustrates the percentage of failures in Phase-2 (IPSec) connections: • The vertical axis shows the average percentage of failed connections in a specific polling cycle. • The horizontal axis shows time of day for the polling cycle.

Monitoring RAS Device Usage and Activity

Performance Monitor provides a high-level overview that shows all of the validated Cisco VPN 3000 Series concentrators that are providing RAS VPN services in any cluster in your network. Use this overview to:

- Isolate data that describe VPN concentrator usage and activity, concentrator failures, and concentrator cryptographic activity.
- View tables and graphs that summarize the condition of any VPN concentrator.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Devices**. For an explanation of the columns in the table, see Table 5-3.

The Remote Access Devices page displays a table of concentrator usage and activity statistics. All measured values on the page are computed as *deltas* (meaning they indicate the scope of difference from one polling cycle to the next)—except for the whole number count of current users.

Note If you or one of your colleagues log out a RAS user, the whole number count of current users might differ the next time the display is refreshed.

Step 2 You can do any of the following to further refine the list or to obtain more detailed information:

- To limit the list to only those devices in a specific cluster, select the cluster in the **Select Cluster** list. Note that Easy VPN does not support the use of RAS clusters.
- To display detailed graphs for one concentrator, click the IP address or DNS name in the Device column.
- To display a graph of dropped packets for one concentrator, click the relevant entry in the Packet Drop % column.
- To display a throughput graph for one concentrator, click the relevant entry in the Throughput (kbps) column.
- To display a graph of bandwidth usage for one concentrator, click the relevant entry in the Bandwidth Usage % column.

Reference

Table 5-3 Remote Access Devices

Element	Description
Alert column	Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe RAS errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14. **Note** After you clear an event, the alert icon continues to be displayed in the device monitoring pages for up to a minute or until the page is refreshed, whichever occurs first.

Table 5-3 Remote Access Devices (continued)

Element	Description
Device column	Displays the device IP address or DNS name. Click any hyperlinked Device column entry to open a new browser that displays your selection as a graph.
Cluster column	Displays the DNS name of the virtual cluster master.
Model column	Displays the Cisco device model name and number.
# Of Users column	Displays the number of active sessions. **Note** If you or one of your colleagues log out a RAS user, this value might differ the next time the display is refreshed.
Packet Drop % column	Displays a computation of the dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all inbound and outbound packets. Click any hyperlinked Packet Drop % column entry to open a new browser that displays your selection as a graph.
Packets In column	Displays the number of inbound packets.
Packets Out column	Displays the number of outbound packets.
Throughput (kbps) column	Displays the sum of outbound and inbound octets through the public interface on the specified RAS device. Click any hyperlinked Throughput (kbps) column entry to open a new browser that displays your selection as a graph.
Bandwidth Usage % column	Displays the percentage of bandwidth used by the specified RAS device, divided by the bandwidth available to it. Click any hyperlinked Bandwidth Usage column entry to open a new browser that displays your selection as a graph.
Last Updated column	Displays the most recent date and time at which Performance Monitor polled the device.

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Monitoring RAS Device Failures

You can display and work from a table that describes the operational failures of your validated VPN concentrators.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Devices > Failures**. For an explanation of the columns in the table, see Table 5-4.

All measured values on the Remote Access Failures page are computed as deltas.

Step 2 You can refine the list and also get more detail:

- To limit the list to only those devices in a specific cluster, select the cluster in the **Select Cluster** list. Note that Easy VPN does not support the use of RAS clusters.
- To display detailed statistics for one VPN concentrator, click the IP address or DNS name in the Device column. See Working with RAS Devices, page 5-4.

Reference

Table 5-4 Remote Access Failures

Element	Description
Alert column	Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe RAS errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.
Device column	Displays the device DNS name or IP address. Click any Device column entry to display performance summary graphs for the selected device.
Inbound Connect Failure % column	Displays the percentage of all inbound connection attempts that failed during Phase-1 (IKE) or Phase-2 (IPSec) and were initiated remotely.
IKE Phase 1 Failure % column	Displays the percentage of Phase-1 (IKE) tunnels that were initiated locally and failed to activate.
IPSec Phase 2 Failure % column	Displays the percentage of received Phase-2 (IPSec) exchanges that were invalid and rejected.
Replays column	Displays the total number of inbound packets dropped (because of anti-replay processing) by all current and previous Phase-2 (IPSec) tunnels.

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Monitoring RAS Device Crypto Activity

You can display and work from a high-level table of cryptographic activity data for validated VPN concentrators.

Note Displayed results do not include the VPN 3005 Concentrator or the VPN 3015 Concentrator. These devices use software encryption instead of scalable encryption processor (SEP) cards.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Devices > Cryptos**. For an explanation of the columns in the table, see Table 5-5.

All measured values on the Remote Access Cryptos page are computed as deltas, except for the whole number count of SEP cards.

Step 2 You can refine the list and also get more detail:

- To limit the list to only those devices in a specific cluster, select the cluster in the **Select Cluster** list. Note that Easy VPN does not support the use of RAS clusters.
- To display detailed statistics for one VPN concentrator, click the IP address or DNS name in the Device column. See Working with RAS Devices, page 5-4.

Reference

Table 5-5 Remote Access Device Cryptos

Element	Description
Alert column	Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe RAS errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.
Device column	Displays the device IP address or DNS name. Click any Device column entry to display performance graphs for the selected device.
No. Cards column	Displays the total number of installed scalable encryption processor (SEP) cards in the monitored device.
Encryption Failure % column	Displays the percentage of outbound encryptions that ended in failure in all currently active Phase-2 (IPSec) tunnels, across all SEP cards.
Decryption Failure % column	Displays the percentage of inbound decryptions that ended in failure in all currently active Phase-2 (IPSec) tunnels, across all SEP cards.
Packet Drop % column	Displays the percentage of dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels across all SEP cards.
Encrypted Packets column	Displays the aggregate number of encrypted, outbound packets across all SEP cards.
Decrypted Packets column	Displays the aggregate number of decrypted, inbound packets across all SEP cards.
Throughput (Kbps) column	Displays the aggregate number of outbound (encrypted) and inbound (decrypted) octets across all SEP cards, in Kbps.

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Viewing RAS Device Crypto Accelerator Card Data

You can display and work from a table of cryptographic accelerator card data for one validated VPN concentrator.

Note Displayed results do not include the VPN 3005 Concentrator or the VPN 3015 Concentrator. These devices use software encryption instead of SEP cards.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Device Details > Crypto Status**. For an explanation of the columns in the table, see Table 5-6.

All measured values on the Remote Access Cryptos page are computed as deltas.

Step 2 Select the device you want to view from the **Select Device** list.

Reference

Table 5-6 Remote Access Cryptos

Element	Description
Slot column	Identifies the number of the slot in the VPN concentrator where the SEP card is installed.
Status column	Displays a message that describes the functional status of the SEP card.
Packets In column	Displays the number of decrypted inbound packets on the SEP card.
Packets Out column	Displays the number of encrypted outbound packets on the SEP card.
Packet Drop % column	Displays the number of dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all decrypted inbound and encrypted outbound packets.
Throughput (Kbps) column	Displays the total number of encrypted outbound and decrypted inbound octets over time on the SEP card.

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Viewing the Remote Access Interfaces Table

You can display and work from a table of interface status data for one validated VPN concentrator.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Device Details > Interfaces**. For an explanation of the columns in the table, see Table 5-7.

The Remote Access Interfaces page displays information about the *public interface* and the *private interface*. A public (outside) interface uses public IP addresses and connects to outside networks. A private (inside) interface uses private IP addresses and is hidden from outside networks.

All measured values on the Remote Access Interfaces page are computed as deltas.

Step 2 Select the device you want to view from the **Select Device** list.

Reference

Table 5-7 Remote Access Interfaces Page

Element	Description
Description column	Provides a specific description of the physical interface, for example, DEC 21143A PCI Fast Ethernet.
Address column	Displays the interface MAC address.
Type column	Displays the frame type to which TCP/IP is bound. For example, a displayed type of iso88023-csmacd indicates a frame type of 100 Mb/s FastEthernet that applies CSMACD (carrier sense multiple access/collision detection).
Access column	Displays either Public or Private.
Admin Status column	Displays Up or Down.
Oper Status column	Displays Up or Down.
Speed (Kbps) column	Displays the interface speed in Kbps.
Packets In column	Displays the total number of inbound packets since the previous polling cycle.
Packets Out column	Displays the total number of outbound packets since the previous polling cycle.
Packet Drop % column	Displays the percentage of packets dropped since the previous polling cycle.
Throughput (Kbps) column	Displays the total number of encrypted outbound and decrypted inbound octets over time on the interface.

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Working with RAS Users

The following topics describe the features with which you monitor RAS users.

- Viewing RAS User Details, page 5-12
- Identifying the Top 10 Users of a RAS Device, page 5-13
- Identifying the Top 10 Users of a RAS Cluster, page 5-14

Viewing RAS User Details

You can isolate and display detailed recent connection information for a single current RAS VPN user. Optionally, you can log out the user you find.

Note Finding a user session might take longer than 1 minute if the relevant VPN concentrator has many active sessions.

Tip You can also display reports that:

- Rank the top 10 RAS VPN users over a range of time that you specify, according to a trending type that you select. See Viewing RAS VPN Top 10 User Reports, page 10-8.
- Describe the VPN sessions of one or more RAS VPN users over a range of time that you specify. See Viewing RAS VPN User Session Reports, page 10-8.

Before You Begin

The user logout feature is available to you only if:

- Your CiscoWorks user role is System Administrator or Network Administrator. See Understanding User Permissions, page 3-2.
- The VPN 3000 Concentrator Series Manager is enabled on the relevant VPN concentrator, and Performance Monitor has a record of the correct authentication credentials for that concentrator.

Procedure

Step 1 Select **Monitor > Remote Access VPN > User Lookup**.

Step 2 Enter the user details:

- **Find User**—Enter the user's IP address or username.
- **Search In**—If desired, you can restrict your search to either one device or one cluster, and identify the search target by selecting its name or IP address. Select Devices All to not restrict the search to a specific device or cluster.

Step 3 Click **Go**. If the user is found, the following user session details are shown:

- User Name—The user's login name.
- Group Name—The user group to which the user belongs.
- Cluster Name—Identifies the cluster by name or IP address, if the VPN concentrator is a cluster member.
- Device Name—Identifies the VPN concentrator by name or IP address.
- Client IP Address—The user's IP address.
- Protocol—The user's connection protocol, such as IPSec over UDP.
- Throughput (Kbps)—The user's average throughput per second.
- Connection Duration—Measured in days, hours, minutes, and seconds.

- Octet In—The total number of inbound octets since tunnel inception.
- Octet Out—The total number of outbound octets since tunnel inception.

Step 4 (**Optional**) To end the user session, click **Logout**.

If the logout is successful, the specified user is logged out and his or her IP address no longer appears in any table that describes active RAS sessions. A system message tells you "The user <username> was logged out successfully."

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Identifying the Top 10 Users of a RAS Device

Performance Monitor can rank the top 10 users who are connected to all validated VPN concentrators or to the validated concentrators in one cluster. The ranking values are determined by throughput, connection duration, or total traffic per user.

Note Performance Monitor ranks the top 10 users on each VPN concentrator. It then ranks only those users against one another when it calculates the top 10 users overall. A user who ranks outside the top 10 for a specific concentrator is excluded from the overall ranking even when the top users for a different concentrator have lower throughput or bandwidth requirements than the excluded user. The top 10 ranking is therefore approximate.

Before You Begin

The user logout feature is available to you only if:

- Your CiscoWorks user role is System Administrator or Network Administrator. See Understanding User Permissions, page 3-2.
- The VPN 3000 Concentrator Series Manager is enabled on the relevant VPN concentrator, and Performance Monitor has a record of the correct authentication credentials for that concentrator.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Device Details > Top 10 Device Users**.

All measured values on the Top 10 Device Users page are whole numbers, rather than deltas. For a description of the table columns, see Table 5-8.

Step 2 Select the device you want to view from the **Select Device** list.

Step 3 Select the ranking criterion for the calculation of top users from the **Compute Using** list. Your options are:

- Throughput—Ranks users according to their throughput, measured in kbps.
- Connect Duration—Ranks users according to the duration of their current session (in days, hours, minutes, and seconds).
- Total Traffic—Ranks users according to the sum of their inbound and outbound packets.

Step 4 If desired, you can disconnect a user. Ending a user session might take longer than 1 minute if the VPN concentrator has many active sessions.

To log out a user, click the radio button for the user, then click **Logout**. If the logout is successful, the user is logged out and his or her IP address no longer appears in any table that describes active RAS sessions.

Reference

Table 5-8 Top 10 Device Users

Element	Description
User column	Displays the username that is associated with the current session. **Note** EzVPN sessions do not support this feature.
Group column	Displays the user group name that is associated with the username. The group name is hyperlinked if the user session is associated with a router that is configured as an Easy VPN server. In this case, you can click the link to open the Details of the Group Policy window. See Details of the Group Policy, page 5-16.
Public IP Address column	Displays the user IP address.
Protocol column	Identifies the protocol in use for the described VPN session.
Traffic In column	Displays the total number of inbound packets.
Traffic Out column	Displays the total number of outbound packets.
Total Traffic column	Displays the combined number of inbound and outbound octets.
Connect Duration column	Displays the number of days, hours, minutes, and seconds since the user established the current session.
Throughput (Kbps) column	Displays the total number of encrypted outbound and decrypted inbound octets over time per user session.

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Identifying the Top 10 Users of a RAS Cluster

You can rank all users that are connected to a cluster, or rank users across all clusters, excluding any Easy VPN users. Easy VPN does not support the use of RAS clusters.

You can also logout one user at a time, excluding any Easy VPN users.

Before You Begin

The user logout feature is available to you only if:

- Your CiscoWorks user role is System Administrator or Network Administrator. See Understanding User Permissions, page 3-2.

- The VPN 3000 Concentrator Series Manager is enabled on the relevant VPN concentrator, and Performance Monitor has a record of the correct authentication credentials for that concentrator.

Procedure

Step 1 Select **Monitor > Remote Access VPN > Top 10 Cluster Users**.

All measured values on the Top 10 Cluster Users page are whole numbers, rather than deltas.

Step 2 Select the cluster you want to view from the **Select Cluster** list. Select All to not restrict the report to a specific cluster.

Step 3 Select the ranking criterion for the calculation of top users from the **Compute Using** list. Your options are:

- Throughput—Ranks users according to their throughput, measured in kbps.
- Connect Duration—Ranks users according to the duration of their current session (in days, hours, minutes, and seconds).
- Total Traffic—Ranks users according to the sum of their inbound and outbound packets.

Step 4 If desired, you can disconnect a user. Ending a user session might take longer than 1 minute if the VPN concentrator has many active sessions.

To log out a user, click the radio button for the user, then click **Logout**. If the logout is successful, the user is logged out and his or her IP address no longer appears in any table that describes active RAS sessions.

Reference

Table 5-9 Top 10 Cluster Users

Element	Description
User column	Displays the authenticated username for the current session.
Group column	Displays the user group name entry that is associated with the named user. The group name is hyperlinked if the user session is associated with a router that is configured as an Easy VPN server. In this case, you can click the link to open the Details of the Group Policy window. See Details of the Group Policy, page 5-16. **Note** The group name is never hyperlinked if the user session is associated with the Easy VPN server on a PIX firewall or a VPN 3000 concentrator.
Public IP column	Displays the user's public IP address.
Protocol column	Identifies which Layer 2 protocol type is used for this VPN session: IPSec, L2TP, or PPTP.
Traffic In column	Displays the number of inbound packets.
Traffic Out column	Displays the number of outbound packets.
Total Traffic column	Displays the combined number of inbound and outbound octets.
Connect Duration column	Displays the number of seconds since the active session began.
Throughput (kbps) column	Displays the number of outbound octets, added to the number of inbound octets, per user session.

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Details of the Group Policy

The following table describes the fields for the group policy that is assigned to a user session when the session is associated with a router that is configured as an Easy VPN server. For information on opening this window, see Identifying the Top 10 Users of a RAS Device, page 5-13 or Identifying the Top 10 Users of a RAS Cluster, page 5-14.

Note No equivalent information is available for Easy VPN sessions that originate from PIX Security Appliances.

Table 5-10 Details of the Group Policy Window

Element	Description
Group Name row	Displays the user group name that is associated with the username in the relevant session.
Pool Name row	Displays the name of the IP local pool address, which defines a range of addresses from which to allocate an internal IP address to a client. Although a user must define at least one pool name, a separate pool may be defined for each group policy. This attribute must be defined and must refer to a valid IP local pool address, or the client connection will fail
DNS Servers row	Displays a comma-separated list of the IP addresses for all of the DNS servers that the specified group uses.
WINS Servers row	Displays a comma-separated list of the IP addresses for all of the WINS servers that the specified group uses.
Domain Name row	Displays the DNS-resolvable domain name that the group uses, such as cisco.com.
ACL row	Sometimes displays the name of an ACL that defines which traffic is to be encrypted. The ACL name is shown only when you configure split-tunneling for the relevant group.
Backup Gateway row	Displays the IP address or hostname of the backup gateway that the router is configured to try first if the connection to the primary Easy VPN server fails.
Firewall Are-U-There row	Shows whether any clients have sent a signal to the server group to indicate that their VPN sessions pass through the Black Ice or Zone Alarm personal firewalls.
Include-local-lan row	Indicates whether an attribute is set for the group that (without the use of split-tunneling) supports simultaneous connections to the client and to a local network—sometimes called a “stub” network—that sends all non-local traffic on the default route 0.0.0.0/0.
Group Lock row	Indicates whether an attribute is set for the server group so that its users can supply Xauth usernames, including a group name, when preshared key authentication uses IKE. **Note** We recommend that clients who use RSA signature authentication mechanisms such as certificates not use the Group-Lock attribute. Instead, such clients should use the User-VPN-Group attribute.
Save Password row	Indicates whether an option is enabled for the server group that allows users to save their XAuth credentials locally on their client PCs.