CHAPTER 6

Monitoring Site-to-Site VPN Services

Site-to-site VPN monitoring provides all the most important indicators of device and tunnel performance at a glance. Performance Monitor also enables you to determine quickly whether site-to-site 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.

Site-to-site VPNs permit connections between:

- An organization's headquarters, remote offices, and branch offices.
- An organization's intranet and its trusted partners, suppliers, customers, or communities of interest.

Performance Monitor monitors site-to-site VPN services in:

- Cisco IOS VPN routers.
- Cisco Catalyst 6500 series switches in which one or more supported services modules are installed.
- Cisco VPN 3000 Series concentrators.
- Adaptive Security Appliances.
- PIX Security Appliances (also known as PIX firewalls).

Note 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. See Understanding Easy VPN, page 5-2.

Tip To troubleshoot common problems with site-to-site VPN services, see the Troubleshooting appendix.

The following topics explain the site-to-site VPN monitoring features:

Understanding DMVPN

The Dynamic Multipoint VPN (DMVPN) feature on Cisco IOS routers provides a simple and scalable way to create large and small IPsec VPNs by combining GRE tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP). In NHRP, the hub maintains a database of public IP addresses for all spokes. Spokes in a DMVPN network register their public IP addresses with the hub during every boot session. Source spokes query the NHRP database on the hub to obtain the public IP address of destination spokes. A multipoint GRE tunnel interface enables a single GRE tunnel to support multiple IPSec tunnels. This method reduces complexity.

DMVPN supports two configurations, *hub-to-spoke* and *spoke-to-spoke*.

- The benefits of a hub-to-spoke deployment include:
  - Simplified and smaller configurations for hub and spoke.
  - Zero-touch provisioning for adding new spokes to the VPN.
  - Support for dynamically addressed spokes.
  - Support for multicast traffic from hub to spokes.
- The benefits of a spoke-to-spoke deployment include all of the benefits from a hub and spoke deployment, plus:
  - Direct dynamic spoke-to-spoke tunnels.
  - Support for participation by smaller spokes in the virtual full mesh.

In addition, Performance Monitor enables you to select a third option, *spoke-to-hub*. Spoke-to-hub is not actually a configuration that you can deploy. Instead, it is a convenience in Performance Monitor that enables you to select a spoke and quickly identify its associated hub.

In Performance Monitor, DMVPN usage is represented in the Tunnels page, where any displayed results are constrained by your selections from the Select Tunnel Type list. See Displaying the Site-to-Site Device Tunnels Table, page 6-9.

Note You might receive a flood of email messages about your DMVPN spoke-to-spoke tunnels if you do *all* of the following:

- Configure DMVPN to use a full mesh topology that supports spoke-to-spoke sessions.
- Configure a threshold for site-to-site VPN tunnel down events.
- Schedule automatic email notification for those events.

Site-to-site tunnels are dynamic and have short lives by design, which include many tunnel down events. If this email flood problem affects you, we recommend that you either disable email notification or configure Performance Monitor to monitor hubs only.

DMVPN and Easy VPN Comparison

The following table describes major differences between DMVPN and Easy VPN. To learn more about Easy VPN and how it is represented in Performance Monitor, see Understanding Easy VPN, page 5-2.

Table 6-1 Comparison of DMVPN and Easy VPN

Service/Feature Name	DMVPN	Easy VPN
Support for multicast traffic	Yes.	—
Spoke-to-spoke communication	Yes.	—
Support for GRE/Quality of Service	Yes.	—
Support for routing protocols	Yes.	—
Support for certificates	Yes.	—
Stateful failover	Depends on routing protocol for recovery.	Yes.
Scalability per hub	Because of routing protocols, DMVPN hubs support fewer spokes per hub.	Supports many spokes per hub.
Identical configuration for all spokes	—	Yes.
Cross-platform support	—	Yes.
Support for software or hardware clients	Hardware client only.	Yes.
Always up tunnel to hub	Yes.	Not required.

Working with Site-to-Site Devices

The following topics explain how you can monitor the status of individual devices and modules that provide site-to-site VPN services.

- Monitoring Site-to-Site Device Usage and Activity, page 6-3
- Monitoring Site-to-Site Device Failures, page 6-4
- Monitoring Site-to-Site Device Crypto Activity, page 6-5

Monitoring Site-to-Site Device Usage and Activity

You can display and work from a table of usage and activity statistics for any of the validated site-to-site devices or service modules in your network. You can view all of your devices or only those in specific groups. You can use this overview to:

- Isolate descriptions of device usage and activity, device failures, and device crypto activity.
- Display charts and graphs that summarize the condition of any device or module that provides site-to-site VPN services.

To view the site-to-site device table, select **Monitor > Site-to-Site VPN > Devices**. For an explanation of the columns in this table, see Table 6-2.

Following are some of the things you can do using this table:

- Display only the devices in one user-defined device group, or display all devices—Select a group name from the Select Group list. The refreshed page lists only the devices in the specified group. The default is to display all devices. Note that some of your monitored devices might not belong to any user-defined device groups.
- Open an Event Browser that displays only the critical errors (P1 or P2) for a specific device or service module—Click the alert icon in the Alert column for the device.

Note The Alert column is empty for a device or module without any critical errors.

- Display charts and graphs that summarize the overall condition of one device or service module—Click the DNS name or IP address in the Device column.
- Display a throughput graph for one device or service module—Click a hyperlinked entry in the Throughput (Kbps) column.
- Display a graph of dropped packets for one device or service module—Click a hyperlinked entry in the Packet Drop % column.

Table 6-2 Site-to-Site Devices Table

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 site-to-site VPN 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.
Device column	Displays the device IP address or DNS name.
Model column	Displays the Cisco device model name.
CPU Usage % column	Displays the average used percentage of total CPU capacity.
Memory Usage % column	Displays the average used percentage of total processor memory capacity since the previous polling cycle.
Throughput (Bps) column	Displays the sum of inbound and outbound octets through the public interface since the previous polling cycle, in bytes.
No. Tunnels column	Displays the combined number of active and inactive tunnels since the previous polling cycle.
Packets In column	Displays the number of packets received through all active Phase-1 (IKE) and Phase-2 (IPSec) tunnels since the previous polling cycle.
Packets Out column	Displays the number of packets sent through all active Phase-1 (IKE) and Phase-2 (IPSec) tunnels since the previous polling cycle.
Packet Drop % column	Displays the number of dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels since the previous polling cycle as a percentage of all such inbound and outbound packets.
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 Site-to-Site Device Failures

To display and work from a table that describes the operational failures of validated site-to-site devices and service modules, select **Monitor > Site-to-Site VPN > Devices > Failures**.

All measured values on the Site-to-Site Failures page are computed as deltas. For a description of the columns, see Table 6-3.

To display charts and graphs that summarize the overall condition of one device or service module in the Failures table, click the relevant DNS name or IP address in the Device column.

Table 6-3 Site-to-Site Device 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 site-to-site VPN 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.
Inbound Connection Failure % column	Displays the inbound Phase-1 (IKE) and Phase-2 (IPSec) connections that were initiated remotely and failed, as a percentage of all connection attempts (inbound and outbound).
Outbound Connection Failure % column	Displays the outbound Phase-1 (IKE) and Phase-2 (IPSec) connections that were initiated locally and failed, as a percentage of all outbound connection attempts.
Replay column	Displays the total number of inbound packets dropped (because of anti-replay processing) by all current and previous IPSec Phase-2 tunnels.
Connection Failure % column	Displays the sum of inbound and outbound connection failures over all exchanges.

Related Topics

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

Monitoring Site-to-Site Device Crypto Activity

To display and work from a table of cryptographic activity on any validated site-to-site device, select **Monitor > Site-to-Site VPN > Devices > Cryptos**.

The Site-to-Site Cryptos page describes the encryption and decryption activities of your VPN routers and IPSec VPN service modules. All measured values on the Site-to-Site Cryptos page are computed as deltas. For a description of the columns, see Table 6-4.

To display charts and graphs that summarize the overall condition of one device or service module in the Crypto Activity table, click the relevant DNS name or IP address in the Device column.

Table 6-4 Site-to-Site Cryptos Page

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 site-to-site VPN errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.

Table 6-4 Site-to-Site Cryptos Page (continued)

Element	Description
Device column	Displays the device DNS name or IP address.
Packet In column	Displays the aggregate number of inbound packets across all SEP cards.
Packet Out column	Displays the aggregate number of outbound packets across all SEP cards.
Packet Drop % column	Displays a computation of the total number of outbound encryptions that ended in failure in all currently and previously active Phase-1 (IKE) and Phase-2 (IPSec) tunnels.
Encrypt Failure % column	Displays the percentage of outbound encryptions that ended in failure in all active Phase-2 (IPSec) tunnels.
Decrypt Failure % column	Displays the percentage of inbound decryptions that ended in failure in all active Phase-2 (IPSec) tunnels.

Related Topics

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

Working with Site-to-Site Device Details

Performance Monitor enables you to display and work from detailed presentations of essential site-to-site VPN device information. See these topics for additional information:

- Displaying and Interpreting Site-to-Site Device Detail Graphs, page 6-6
- Displaying the Site-to-Site Device Interfaces Table, page 6-8
- Displaying the Site-to-Site Device Tunnels Table, page 6-9

Displaying and Interpreting Site-to-Site Device Detail Graphs

You can display a graphical representation of the status of any validated device in any of your site-to-site VPNs.

Procedure

Step 1 Select **Monitor > Site-to-Site VPN > Device Details**.

Initially, Performance Monitor 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 6-5.

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 Site-to-Site Graphs

Table 6-5 Types of Site-to-Site Device Graphs

Graph Type	Description
CPU Usage	Illustrates the used percentage of device CPU capacity: • The vertical axis shows the average percentage of CPU capacity used in a specific polling cycle. • The horizontal axis shows the time of day for the polling cycle.
Memory Usage	Illustrates the used percentage of device memory capacity: • The vertical axis shows the average percentage of memory capacity used in a specific polling cycle. • The horizontal axis shows the time of day for the polling cycle.
Packet Drops	Illustrates the percentage of dropped packets in site-to-site VPN tunnels: • The vertical axis shows the average percentage of dropped packets in a specific polling cycle. • The horizontal axis shows time of day for the polling cycle.
Throughput vs. No. Tunnels	Displays a line graph that helps you compare throughput trends to the trend of the number of tunnels in use 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 for a specific polling cycle, in bytes per second. – The vertical axis on the right (blue) shows the average number of tunnels in a specific polling cycle. • The horizontal axis shows the time of day at which Performance Monitor calculated the trends in each vertical axis.
Inbound Connection 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 the time of day for the polling cycle.
Outbound Connection Failures	Illustrates the trend of outbound connection failures over time: • The vertical axis shows the average number of failures in a specific polling cycle. • The horizontal axis shows the time of day for the polling cycle.

Related Topics

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

Displaying the Site-to-Site Device Interfaces Table

You can display and work from a table of site-to-site device interface performance and activity statistics.

Procedure

Step 1 Select **Monitor > Site-to-Site VPN > Device Details > Interfaces**. For an explanation of the columns in the table, see Table 6-6.

The Site-to-Site Interfaces page describes device interfaces that are either bound to a crypto map or that are of Internet Assigned Number Authority (IANA) interface type 131—tunnel.

All measured values on the Site-to-Site Interfaces page are computed as deltas.

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

By default, only the VPN interfaces are listed in the table. However, you can select All Interfaces from the Select Interfaces list to see all of the interfaces for the device.

Reference

Table 6-6 Site-to-Site Interfaces Page

Element	Description
Descr column	Provides a specific description of the physical interface. For example, DEC 21143A PCI Fast Ethernet.
Address column	Displays the interface MAC address.
Admin Status column	Displays either Up or Down.
Operation Status column	Displays either Up or Down.
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 MBits/s FastEthernet that applies CSMACD (carrier sense multiple access/collision detection).
Speed (Kbps) column	Displays the interface speed in Kbps.
Packet In column	Displays the total number of packets received on the interface since the previous polling cycle.
Packet Out column	Displays the total number of packets sent from the interface since the previous polling cycle.
Packet Drop % column	Displays the total percentage of packets dropped since the previous polling cycle.
Throughput (Bps) column	Displays the average interface throughput rate in bytes.

Related Topics

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

Working with Site-to-Site Tunnels

The following topics describe ways to work with tunnels in site-to-site VPNs.

Displaying the Site-to-Site Device Tunnels Table

You can display and work from a table of VPN tunnels on all of your validated site-to-site devices, or display the tunnels on one device.

To display the list of tunnels, select **Monitor > Site-to-Site VPN > Device Details > Tunnels**.

By default, the Tunnels page describes tunnels on all of your validated site-to-site devices. The displayed values are whole numbers, computed since tunnel inception.

You can filter the list using the drop-down lists above the table:

- Select Device—Select the IP address of a device to display information about VPN tunnels on that device.
- Select Tunnel Type—Select a DMVPN tunnel type for viewing, or view all site-to-site tunnels, or learn which hub a device uses.
  - All— View all DMVPN tunnels for the selected device.
  - DMVPN Hub-Spoke—View only the hub-to-spoke DMVPN tunnels for the selected device.
  - DMVPN Spoke-Hub—This option is a convenience in Performance Monitor that enables you to quickly identify which hub is associated with a spoke that you select from the Select Device list.
  - DMVPN Spoke-Spoke—View only the spoke-to-spoke DMVPN tunnels. These tunnels are dynamic and can have very short lifetimes that generate many tunnel up and tunnel down events.

The following table describes the columns in the tunnels table.

Table 6-7 Tunnels Page

Element	Description
Local Endpoint column	Displays the IP address of the local endpoint device interface at which the tunnel terminates. In the case of a DMVPN tunnel, you can click the hyperlinked IP address to see the remote IP address and the time at which the tunnel is scheduled to expire. **Note** The identity of the "local" endpoint device might vary in Performance Monitor, because its definition is always relative to the device that you monitor.
Remote Endpoint column	Displays the IP address of the remote endpoint device interface at which the tunnel terminates. **Note** The identity of the "remote" endpoint device might vary in Performance Monitor, because its definition is always relative to the device that you monitor.
Local Subnet column Remote Subnet column Protocol column	Taken together, the values in these three columns define the access list for one tunnel: • Local Subnet—Displays the tunnel subnet and mask on the local endpoint device. • Remote Subnet—Displays the tunnel subnet and mask on the remote endpoint device. • Protocol—Displays the tunnel protocol and the port used, such as TCP 80.

Table 6-7 Tunnels Page (continued)

Element	Description
Status column	Displays either Up or Down.
Active Time column	Displays the tunnel lifetime in hours, minutes, and seconds.
Auth Fail In column	Displays the number of authentication failures for inbound packets since tunnel inception.
Auth Fail Out column	Displays the number of authentication failures for outbound packets since tunnel inception.
Packets In column	Displays the number of inbound packets since tunnel inception.
Packets Out column	Displays the number of outbound packets since tunnel inception.
Packet Drop % column	Displays dropped packets as a percentage of all inbound and outbound packets since tunnel inception.
Throughput (Bps) column	Displays the sum of inbound and outbound octets through the tunnel since tunnel inception, in bytes.
Last Update 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

Finding a Site-to-Site VPN Tunnel

You can locate, isolate, and display the properties of a single tunnel.

Procedure

Step 1 Select **Monitor > Site-to-Site VPN > Tunnel Lookup**.

The Site-to-Site Tunnel Lookup page appears.

Step 2 To identify one tunnel, enter:

- The IP address of the endpoint device interface at which one end of the tunnel terminates.
- The IP address of the endpoint device interface at which the *opposite end* of the *same* tunnel terminates.

Step 3 Click **Go**. If the tunnel is found, the page displays the details for the tunnel. For an explanation of the columns, see Displaying the Site-to-Site Device Tunnels Table, page 6-9.

Related Topics

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