VPN Monitoring and Troubleshooting in Security Cloud Control

- Monitor site-to-site VPNs using Site-to-Site VPN summary page, on page 1
- Monitor Remote Access VPN Sessions, on page 1
- SD-WAN summary dashboard, on page 1

Monitor site-to-site VPNs using Site-to-Site VPN summary page

You can view a summary of your site-to-site VPN topologies in the **Site-to-Site VPN Summary** page. For each topology, you can view details such as VPN type, network topology, VPN interfaces, VPN devices, and tunnel statuses.

You can edit or delete the topology using the edit and delete buttons. For SASE topology VPNs, you have options to deploy, edit and delete any topology.

Monitor Remote Access VPN Sessions

The Security Cloud Control Remote Access Monitoring dashboard can be used to view consolidated information about RA VPN users, including the current status of users, device types, client applications, user geolocation information, and duration of connections. You can also disconnect RA VPN sessions as needed.

See Monitor Remote Access Virtual Private Network Sessions for more information.

SD-WAN summary dashboard

The SD-WAN Summary dashboard (**Insights & Reports** > **VPN dashboards** > **SD-WAN SummaryAnalysis** > **SD-WAN Summary**) provides a snapshot of your WAN devices and their interfaces. This dashboard helps you to:

- Identify issues with the underlay and overlay (VPN) topologies.
- Troubleshoot VPN issues using the existing **Health Monitoring**, **Device Management**, and **Site-to-Site Monitoring** pages.

- Monitor application performance metrics of WAN interfaces. The threat defense steers application traffic based on these metrics.

For clusters, this dashboard displays application performance metrics of only the control node and not the data nodes.

WAN device criteria

A WAN device must meet one of these criteria:

- The device must be a VPN peer.
- The device must have WAN interface.

WAN interface criteria

A WAN interface must meet one of these criteria:

- The interface has IP address-based path monitoring enabled on it.
- The interface has a Policy Based Routing (PBR) policy with at least one application configured to monitor it.

For more information about PBR policy and path monitoring, see Policy-Based Routing.

Uplink decisions

Click **Uplink Decisions** to view the **VPN Troubleshooting** page. You can view syslogs with ID: 880001. These syslogs show the threat defense interfaces through which it steers traffic based on the configured PBR policy.

To view the above syslogs and to view the data on this dashboard, ensure that you review Prerequisites for using SD-WAN summary dashboard.

Prerequisites for using SD-WAN summary dashboard

Ensure that you review these prerequisites before using the SD-WAN summary dashboard.

General prerequisites

- You must be an Admin, Security Analyst, or Maintenance user to view this dashboard. See Secure Firewall Management Center and Cloud-delivered Firewall Management Center User Role Mapping for more information.
- Threat Defense devices must be Version 7.2 or later.
- Enable IP-based path monitoring and HTTP-based application monitoring on the WAN interfaces.

  To do this:

  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click the edit icon adjacent to the interface that you want to edit.

4. Click the **Path Monitoring** tab.
5. Check the **Enable IP based Monitoring** check box.
6. Check the **Enable HTTP based Application Monitoring** check box.
7. Click **OK**.

- Configure a PBR policy with at least one application configured to monitor it:
  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click **Routing**.
  4. In the left pane, click **Policy Based Routing**.
  5. Click **Add**.
  6. From the **Ingress Interface** drop-down list, choose an interface.
  7. Click **Add** to configure a forwarding action.
  8. Configure the parameters.
  9. Click **Save**.

- To view syslogs when you click **Uplink Decisions**, you must:
  - Choose **Devices** > **Platform Settings** and create or edit a threat defense policy.
  - In the left pane, click **Syslog**.
  - Click the **Logging Setup** tab.
  - Check the **Enable Logging** check box to turn on the data plane system logging for the threat defense device.
  - Click the **All Logs** radio button to enable logging of all the troubleshooting syslog messages.

    or

    Click the **VPN Logs** radio button to enable logging of only the VPN troubleshooting messages.
  - Click **Save**.

Monitor WAN devices and interfaces using the SD-WAN summary dashboard

The SD-WAN Summary dashboard has these widgets :

- WAN connectivity, on page 4
- VPN topology, on page 4
- interface throughput, on page 4
- Device inventory, on page 4

• WAN device health, on page 4

WAN connectivity

This widget provides a summary of the WAN interfaces statuses. It shows the number of WAN interfaces that are in the **Online**, **Offline** or **No Data** states. Note that you cannot monitor subinterfaces using this widget.

Click **View All Interfaces** to view more details about the interfaces in the health monitor page.

If a WAN interface is in the **Offline** or **No Data** state, you can troubleshoot it from the health monitor page:

1. In the **Monitoring** pane, expand **Devices**.
2. Click the corresponding WAN device to view the device-specific health details.
3. Click the **Interface** tab to view the interface status and aggregate traffic statistics for a specific time.

   Alternatively, you can click **View System & Troubleshoot Details**. The health monitor page is displayed with all the necessary details.

VPN topology

This widget provides a summary of the site-to-site VPN tunnel statuses. It shows the number of **Active**, **Inactive**, and **No Active Data** VPN tunnels.

Click **View All Connections** to view the VPN tunnel details in the **Site-to-site VPN Monitoring** dashboard.

If the tunnels are in the **Inactive** or **No Active Data** state, you can troubleshoot using the **Site-to-site VPN Monitoring** dashboard. In the **Tunnel Status** widget, hover your cursor over a topology, click **View** ( ) and do one of these actions:

- Click the **CLI Details** tab to view the details of the VPN tunnels.
- Click the **Packet Tracer** tab to use the packet tracer tool for the topology.

interface throughput

This widget monitors the average throughput of the WAN interfaces during the chosen time period.

The interface throughput is classified into four bands. These details aid in cost planning and resourcing. You can choose a time range for the widget data from the **Show Last** drop-down list. The range is from 15 minutes to two weeks.

Click **View Health Monitoring** to view more details about the interface in the health monitor page.

Device inventory

This widget lists all the managed WAN devices and groups them according to the model.

Click **View Device Management** to view more details about the device in the **Device Management** page.

WAN device health

This widget displays the device count according to the health of the WAN devices. You can view the number of devices with errors, warnings, or those that are in **Disabled** state.

Click **View Health Monitoring** to view the alarms, and quickly identify, isolate, and resolve issues.

If the health of a device is affected, you can troubleshoot it from the health monitor page.

1. In the **Monitoring** pane, expand **Devices**.
2. Click the corresponding WAN device to view the device-specific health details.
3. Click **View System & Troubleshoot Details**. The health monitor page is displayed with all the necessary details.

A device can be in **Disabled** state for multiple reasons, including these:

- Management interface is disabled.
- Device is powered off.
- Device is being upgraded.

Monitor application performance metrics of WAN interfaces using SD-WAN summary dashboard

You can monitor application performance metrics of WAN interfaces using the **Application Monitoring** tab of the SD-WAN Summary dashboard. These metrics include Jitter, Round Trip Time (RTT), Mean Opinion Score (MOS), and Packet Loss.

By default, the metrics data is refreshed every 5 minutes. You can change the refresh time; the range is from 5 to 30 minutes. You can view the metrics in tabular and graphical formats. For each WAN interface, the latest metric value appears in the table. For graphical data, you can choose a time interval of up to 24 hours to view the metrics data for the corresponding WAN interfaces.