Configure Firewall and SD-WAN Usage Monitoring Controls

For supported software information, click here.

When you enable log export functionality (LEF) statistics logging for firewall and SD-WAN, a Versa Operating System^{TM} (VOS^{TM}) CPE device performs usage monitoring of firewall and SD-WAN traffic activity and exports various categories of usage statistics to Analytics nodes.

For the firewall service, the statistics for usage monitoring are aggregated for each unique source and destination IP address for each tenant.

For the SD-WAN service, the statistics for usage monitoring are aggregated for each unique combination of tenant, application, source IP address, and access circuit. You can configure a VOS CPE device to also export the destination IP address.

By default, a CPE exports all aggregated usage monitoring records up to a maximum of 16,384 (16K) records every 5 minutes.

For CPE devices that carry large amounts of active traffic, the number of unique source and destination IP addresses and the number of applications can be very large. In these cases, exporting all the statistics logs every 5 minutes can result in performance issues, such as overutilization of WAN links; excessive consumption of storage, memory, and CPU on the Analytics nodes; and, occasionally, loss of critical logs because of a burst of log traffic. For these CPE devices, you can reduce the number of firewall and SD-WAN statistics log records that they export, by exporting logs only for the busiest traffic flows. The "busy"-ness is defined by considering a combination of the traffic volume and the number of flows using unique source and destination IP addresses.

To reduce the number of exported statistics log records, you specify the maximum number of log records to export per category or report type. For the busiest CPE devices, it is recommended that you reduce the number of logs to a smaller number every 5 minutes. Then, for that report type, the CPE device exports statistics for that number of records that have the highest traffic volume and highest amount of session activity. These records are sometimes referred to as the *top* records.

Note that the export interval of 5 minutes is fixed and is not user-configurable.

Configure the Exporting of Log Records

To configure the exporting of log records for statistics related to firewall and SD-WAN operations:

1. In Director view:

    a. Select the Configuration tab in the top menu bar.

    b. Select Devices > Devices in the horizontal menu bar.

    c. Select a tenant in the left menu bar.

    d. Select a device in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.

3. Select Others ⚙ > System > Configuration > Configuration in the left menu bar.

4. In the Parameters pane, click the ✏ Edit icon.
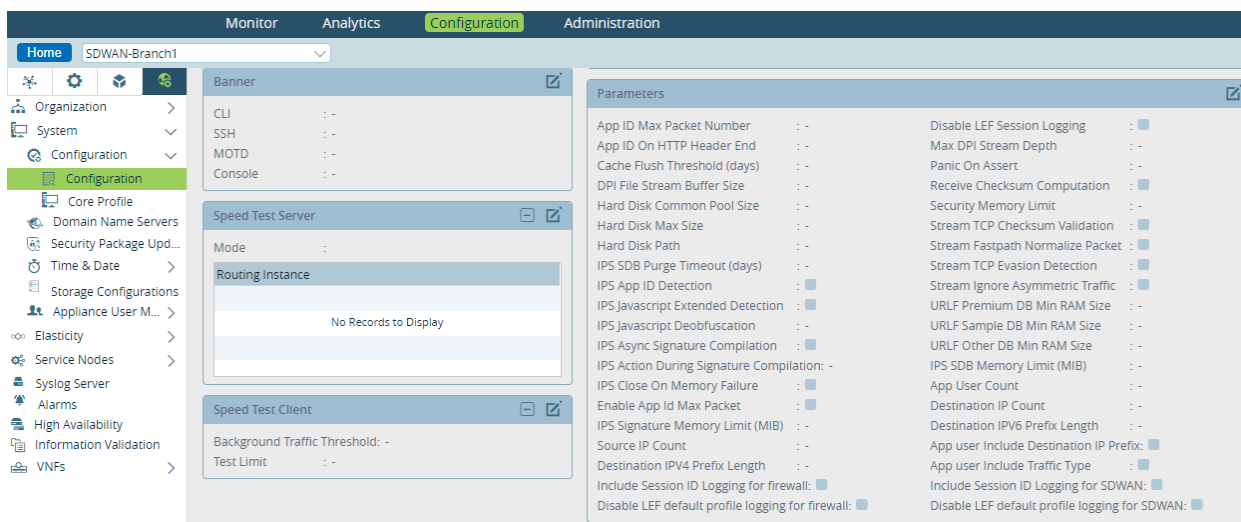
5. In the Edit Parameters popup window, select the LEF tab and then enter information for the following fields.

Field	Description
Firewall (Group of Fields)	Configure the firewall statistics logs to export from the VOS device to the Analytics node.
◦ Source IP Count	Enter the maximum number of unique source IP addresses to export. If you set the value to 0, all source IP address log records are exported. *Range:* 0 through 8192 (for Releases 21.1.1 and later); 0 through 8096 (for Releases 21.1.0 and earlier) *Default:* 50 (for Releases 21.1.1 and later); no default value for Releases 21.1.0 and earlier
◦ Destination IP Count	Enter the maximum number of unique destination IP addresses to export. If you set the value to 0, all destination IP address log records are exported. *Range:* 0 through 8192 (for Releases 21.1.1 and later); 0 through 8096 (for Releases 21.1.0 and earlier) *Default:* 50 (for Releases 21.1.1 and later); no default value for Releases 21.1.0 and earlier

| Field	Description
◦ Include Session ID Logging	Click to include session identification parameters in the exported firewall statistics log. For more information, see [Configure the Exporting of Session Log Records.](#)
SD-WAN (Group of Fields)	Configure the SD-WAN user application statistics logs to export from the VOS device to the Analytics node.
◦ Application User Count	Enter the maximum number of unique user applications to export. If you set the value to 0, all application user log records are exported. *Range:* 0 through 8192 (for Releases 21.1.1 and later); 0 through 8096 (for Releases 21.1.0 and earlier) *Default:* 100 (for Releases 21.1.1 and later); no default value for Releases 21.1.0 and earlier
◦ Destination IPv4 Prefix Length	Enter the destination IP prefix length instead of using the full IPv4 address. This option is useful for SD-WAN log records that include destination IP addresses, such as application performance monitoring (APM). *Value:* 1 through 32 *Default:* 24
◦ Destination IPv6 Prefix Length	Enter the destination IP prefix length instead of using the full IPv4 address. This option is useful for SD-WAN log records that include destination IP addresses, such as APM. *Value:* 1 through 128 *Default:* 64
◦ Application User Include Destination IP Prefix	Click to include the application's destination IP address or prefix in the exported statistics log. This is the destination IP address or prefix that was accessed by a source IP address. By default, the statistics that the VOS branch or hub aggregates for SD-WAN application user usage reports include the following for each tenant: source IP address, application identifier, and access circuit.

Field	Description
◦ Include Session ID Logging	(For Releases 21.1.1 and later.) Click to include session identification parameters in the exported SD-WAN statistics log. For more information, see Configure the Exporting of Session Log Records.

6. Click OK.

7. Click Home to return to Director view.

View Exported Log Records

To view the log records that are exported to an Analytics node:

1. In Director view, select the Analytics tab. The view changes to Analytics view.

2. Select Home > Dashboards in the left menu bar.

3. To identify the users with the largest number of sessions and sending and receiving the highest volume of traffic:

   a. Select SD-WAN > Sites in the left menu bar.

   b. Select the Usage tab in the main pane. The graph at the top of the pane displays usage statistics for the top number of sites.
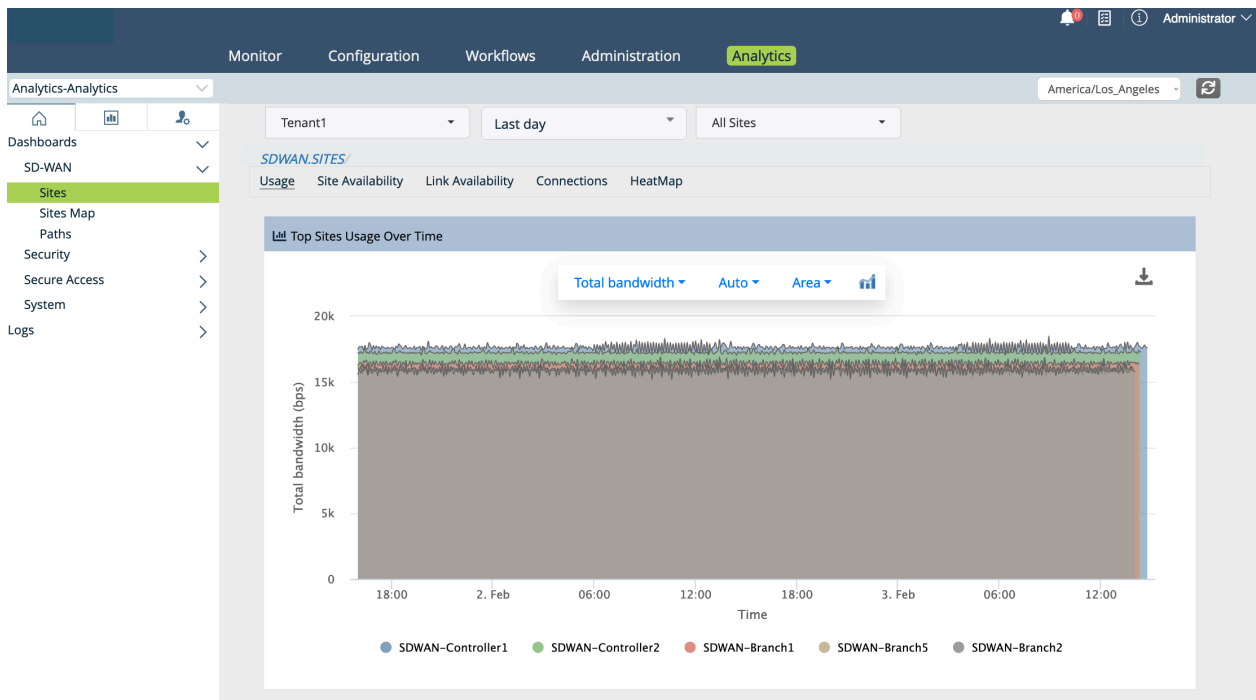
The table at the bottom of the pane displays usage statistics for the top number of sites in tabular format.

4. To view the top statistics for firewalls:

   a. Select Security > Firewall in the left menu bar.

   b. Select the Source tab in the main pane. The table displays usage statistics for the top number of source IP addresses.

   c. Select the Destination tab in the main pane. The table displays usage statistics for the top number of destination IP addresses.

Supported Software Information

Releases 20.2.1 and later support all content described in this article, except:

- Releases 21.1.1 and later change the allowable range and adds default values for the Firewall Source IP Count and Destination IP Count fields, and for the SD-WAN Application User Count field.

Additional Information

Configure Application Performance Monitoring

Configure the Exporting of Session Log Records

Configure Log Export Functionality

Versa Analytics Scaling Recommendations