VPN Monitoring for Firepower Threat Defense

This chapter describes Firepower Threat Defense VPN monitoring tools, parameters, and statistics information.

- VPN Summary Dashboard, on page 1
- VPN Session and User Information, on page 2
- VPN Health Events, on page 3

VPN Summary Dashboard

Firepower System dashboards provide you with at-a-glance views of current system status, including data about the events collected and generated by the system. You can use the VPN dashboard to see consolidated information about VPN users, including the current status of users, device types, client applications, user geolocation information, and duration of connections.

Viewing the VPN Summary Dashboard

Remote access VPNs provide secure connections for remote users, such as mobile users or telecommuters. Monitoring these connections provides important indicators of connction and user session performance at a glance.

You must be an Admin user in a leaf domain to perform this task.

Procedure

Step 1 Choose **Overview** > **Dashboards** > **Access Controlled User Statistics** > **VPN**.

Step 2 View the Remote Access VPN information widgets:

- Current VPN Users by Duration.
- Current VPN Users by Client Application.
- Current VPN Users by Device.
- VPN Users by Data Transferred.
- VPN Users by Duration.
- VPN Users by Client Application.
- VPN Users by Client Country.

What to do next

The VPN dashboard is a complex, highly customizable monitoring feature that provides exhaustive data.

- For complete information on how to use dashboards in the Firepower System, see Dashboards.
- For information on how to modify the VPN dashboard widgets, see Configuring Widget Preferences.

VPN Session and User Information

The Firepower System generates events that communicate the details of user activity on your network, including VPN-related activity. The Firepower System monitoring capabilities enable you to determine quickly whether remote access 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 remote access VPN users as needed.

Viewing Remote Access VPN Active Sessions

Analysis > **Users** > **Active Sessions**

Lets you view the currently logged-in VPN users at any given point in time with supporting information such as the user name, login duration, authentication type, assigned/public IP address, device details, client version, end point information, throughput, bandwidth consumed group policy, tunnel group etc. The system also provides the ability to filter current user information, log users out, and delete users from the summary list.

Note If you have configured your VPN in a high-availability deployment, the device name displayed against active VPN sessions can be the primary or secondary device that identified the user session.

- To learn more about active sessions; see Viewing Active Session Data.
- To learn more about the contents of the columns in the active sessions table; see Active Sessions, Users, and User Activity Data.

Viewing Remote Access VPN User Activity

Analysis > **Users** > **User Activity**

Lets you view the details of user activity on your network. The system logs historical events and includes VPN-related information such as connection profile information, IP address, geolocation information, connection duration, throughput, and device information.

- To learn more about user activity; see Viewing User Activity Data.
- To learn more about the contents of the columns in the user activity table; see Active Sessions, Users, and User Activity Data.

VPN Health Events

The Health Events page allows you to view VPN health events logged by the health monitor on the Firepower Management Center. When one or more VPN tunnels between Firepower System devices are down, these events are tracked:

- VPN for 7000 & 8000 Series
- Site-to-site VPN for Firepower Threat Defense
- Remote access VPN for Firepower Threat Defense

See Health Monitoring for more details on how you can use the health monitor to check the status of critical functionality across your Firepower System deployment.

Viewing VPN Health Events

When you access health events from the Health Events page on your Firepower Management Center, you retrieve all health events for all managed appliances. You can narrow the events by specifying the module which generated the health events you want to view.

You must be an Admin, Maintenance User, or Security Analyst to perform this task.

Procedure

Step 1 Choose **System** > **Health** > **Events**.

Step 2 Select **VPN Status** under the **Module Name** column.

See Health Event Views for more details on system health events.