Network Security Manager Reporting and Analytics

Administration Guide

SONICWALL®

Contents

About Reporting and Analytics **5**
NSM Advanced and Essential Licenses 5
Understanding Analytics 6
Conventions 7
Guide Conventions 7
UI Conventions 8
Related Documents 8
Navigation 9

Manager View **10**
NSM SaaS HOME Dashboard 10
MONITOR Features 11

Group and Tenant Reporting **13**
Understanding How the NSM License Affects Reporting 13
When You Have a Firewall Essential License 13
When You Have a Firewall Advanced License 14
Navigating Reports 15
Tenant Reports 16
Summary Reports 16
Detail Reports 17
Tenant Analytics 18
Group Reports 19
Summary Reports 19
Detail Reports 20
Group Analytics 21

Firewall View **23**
Live Monitoring, Live Report and Up Time Report 23
Live Monitor 23
Live Report 26
Up Time Report 29
Reports and Analytics 29
NSM - Advanced 30
Applications 30
Users 31
Viruses 32

Intrusions 33
Spyware 34
Web Categories 35
Sources 36
Destinations 37
Locations 38
Blocked 38
Threats 39
VPN Reports 40
Navigating the VPN Reports 40

Analytics 44
About Analytics 44
Navigating to the Analytics Page 45
List View 45
Graph View 46
Log View 47
Custom Filters 50
Creating Custom Filters 50
Editing and Deleting Custom Filters 51

Log Download 53
Creating Log Download Rule 53
Downloading Log File 57

Productivity Reports 59
Productivity Groups 59
Navigating to the Productivity Reports Page at Tenant Level 61
Users 63
Websites 66
Web Categories 68

Reports 71
Capture Threat Assessment (CTA) Report Rules 71
Navigating the CTA Report Rules Page 72
Setting Up the CTA Report Rule 72
Default Report Rules 75
Managing Default Reports 75
Navigating the Default Report Rules Page 75
Setting Up the Report Rule 75
Firewall Up-Time Summary Report Rules 79
Navigating the Firewall Up-Time Summary Report Rules Page 79
Setting Up the Firewall Up-Time Summary Report Rule 80
Custom Reports 83

Creating Custom Filters 83
Navigating the Custom Reports Page 83
Generating and Downloading the Report 88

Alerts and Notifications 90
Rules 90
VPN Tunnel Status Alert 91
History 92

Logs 93
System Logs 93
Navigating to System Logs Page 93
Enabling System Logs for Existing Firewalls 95
Authentication Logs 98
Auditing Logs 100

Notification Center 101

SonicWall Support 105
About This Document 106

1

About Reporting and Analytics

SonicWall Analytics can be used in conjunction with NSM SaaS. This allows users to manage firewalls from NSM and also view reporting and analytics data in NSM. A SaaS-based analytics license can be upgraded to include reporting and analytics. When you click on the firewall whose data is stored in Analytics, NSM fetches the data securely from the back-end. Data is encrypted and compressed so that no data integrity issues are experienced.

For SonicWall on-premises NSM does not have integrated Analytics and Reporting at this time. You can add reporting and analytics functionality by installing Analytics On-Premise product (IPFIX or Syslog), along with the on-premises NSM. Contact your sales representative for assistance and refer to the On-Premises Analytics Getting Started Guide and the SonicWall Analytics Administration.

Analytics includes a broad range of predefined reports, as well as the flexibility to create custom reports using any combination of auditable data for thorough risk analysis. These reports combined give detailed insights of network events, user activities, threats, operational and performance issues, security efficacy, risks and security gaps, compliance readiness, and auditing.

NSM Advanced and Essential Licenses

This document covers NSM Advanced and Essential licenses for NSM SaaS offering.

- NSM Advanced comes with Management, 365-days of Reporting and 30-days of Analytics.
- NSM Essential license comes with Management and 7-day of limited Reporting.

The table below lists the available reports in NSM Advanced and NSM Essential License.

NSM ADVANCED	NSM ESSENTIAL
• Productivity • Live Monitor • Live Report • Firewall Up-time Report • Analytics • System Events • Authentication Logs • Alert and Notification • Log Downloads • Applications • Viruses • Intrusions • Spyware • Botnet • Web Categories • Sources • Destinations • Source Locations • Destination Locations • Blocked • Threats • Source VPN • Destination VPN	• Applications • Viruses • Intrusions • Spyware • Web Categories • Addresses • Locations • Firewall Up-time Report

NOTE: Analytics and some Reporting features discussed in this document will not be available in NSM Essential licenses.

Understanding Analytics

Analytics is designed to evaluate data collected by the firewall ecosystem, make policy decisions and take defensive actions using application- and user-based analytics.

SonicWall Analytics extends security event analysis and reporting by providing real-time visualization, monitoring and alerts based on the correlated security data. You can perform flexible drill-down and gain insight into your network, user access, connectivity, application use, threat profiles, and other firewall-related data.

Analytics provides the following key features:

- Data collection that includes normalizing, correlating, and contextualizing the data to the environment
- Streaming analytics in real time
- Analytics including activity trends and connections across the entire network
- Real-time, dynamic visualization of the security data from a single point
- Real-time detection and remediation

SonicWall Analytics is flexible and designed to integrate into other SonicWall solutions:

- On-Premises Analytics can be integrated with on-premises NSM for those customers requiring long term storage of firewall logs and supports designated SonicWall firewalls.

Conventions

About Network Security Manager makes use of the following conventions:

- Guide Conventions
- UI Conventions

Guide Conventions

The following text conventions are used in this guide:

Convention	Use
Bold text	Used in procedures to identify elements in the user interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Menu view or mode | Menu item > Menu item	Indicates a multiple step menu choice on the user interface. For example, **Manager View | HOME > Firewall > Groups** means that you are in the Manager View with the **HOME** option selected. Then click on **Firewall** in the left-hand menu, and select **Groups**.
`Computer code`	Indicates sample code or text to be typed at a command line.
`<Computer code italic>`	Represents a variable name when used in command line instructions within the angle brackets. The variable name and angle brackets need to be replaced with an actual value. For example in the segment *serialnumber=<your serial number>*, replace the variable and brackets with the serial number from your device: serialnumber=C0ABC00000321.
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

UI Conventions

When acquiring devices for management and reporting, the Status option uses colored icons to indicate the various states of the devices being monitored and managed.

Status Icon	Definition
	Indicates that a process is in progress. In some instances, specific details are provided: for example, Requesting Licenses.
	Indicates that a process has completed successfully. May provide the message Success or something with more detail like Device parameters set up in Cloud Capture Security Center complete.
	Indicates that a task is in process or pending the completion of another task. The message Pending is usually displayed, as well.
	Indicates a potential issue. Messages provide additional detail to help you resolve the issue.
	Indicates an error. Additional information may be provided via an information icon. Click the icon or mouse over it to see the message: For example, Gateway Firewall is not available in CSC.
	Indicates the device is online.
	Indicates the device is offline.
	Indicates unmanaged devices.
	Indicates managed devices.

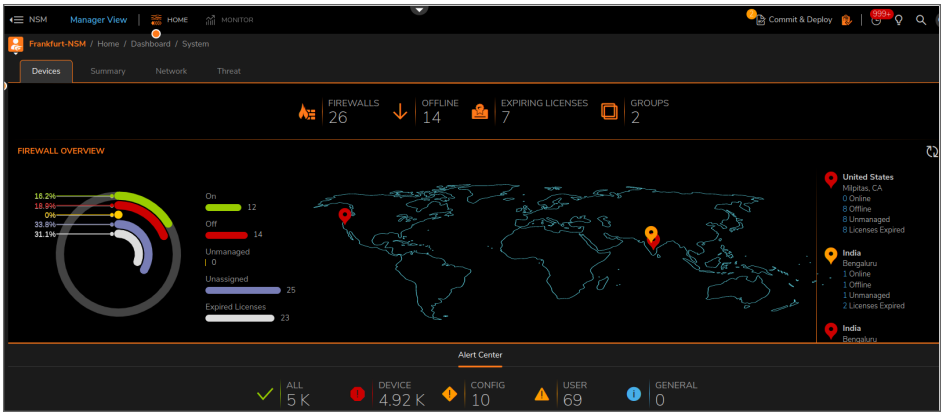
Related Documents

The NSM documentation includes the following:

- *About NSM* provides an overview of the product and describes the base modes of operation, the navigation and icons, and the **Notification Center**.
- The *NSM Getting Started Guide* describes how to license and configure a basic NSM setup.
- The *NSM Administration Guide* reviews the management tasks for administering your security infrastructure.
- The *NSM Release Notes* summarizes the new features for the product.

Navigation

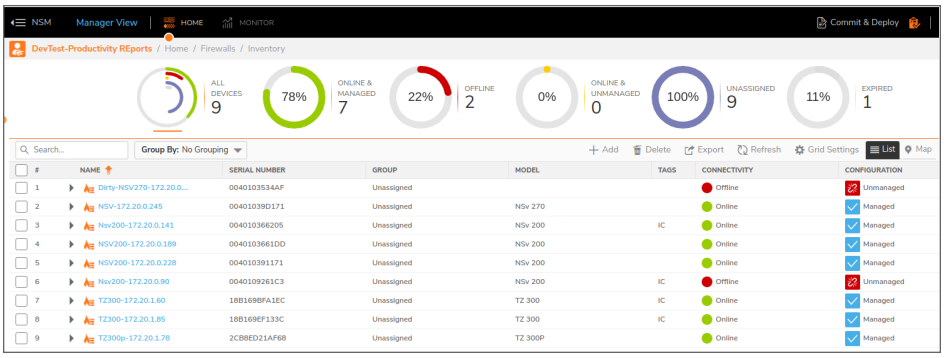
The interface for Analytics varies because of the different configurations and types of reporting that can be selected. When you log in to NSM, it takes you to the Dashboard view, where you can see Analytics data like **Devices**, **Summary**, **Network**, and **Threat**. Click **MONITOR** to access other Analytics and Reporting features.



The **MANAGER VIEW** does not show **Live Monitor** and **Alerts & Notifications** features. To access Analytics features for specific firewalls, you have to select **FIREWALL VIEW**.

To navigate to FIREWALL VIEW:

1. In **MANAGER VIEW**, select **HOME**.
2. Click **Firewall > Inventory**.



3. Select the firewall you want to monitor to see the dashboard for that specific device.
4. Click **HOME** icon at the top and select **MONITOR** from the drop-down list to see the reports available for that same device.

2

Manager View

This section describes the dashboards of both NSM on-premises and SaaS versions.

NSM SaaS HOME Dashboard

In **MANAGER VIEW** you can access Dashboard and Reporting statistics along with summarized trends of all the connected firewalls in your network infrastructure.

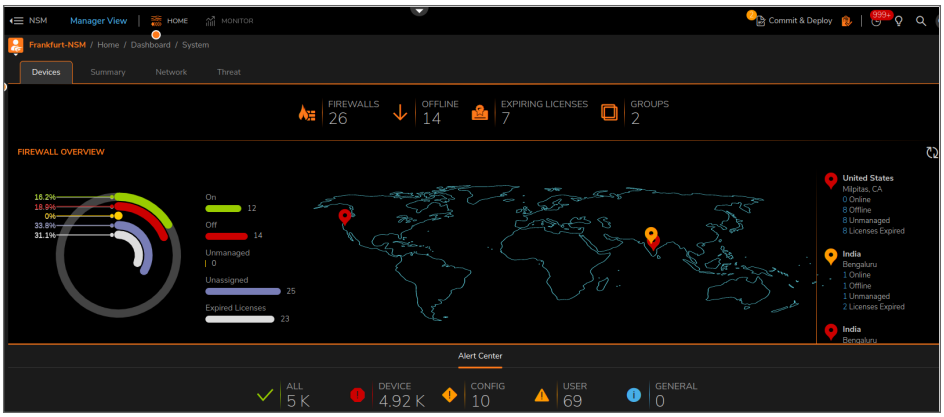
Dashboard enables you to visualize status of the security infrastructure, assess the performances, and monitor the issues that need investigation, at a glance. The analytical dashboard NSM provides is an optimal solution to quickly analyze the cyber security risks and recognize how to resolve them.

NSM dashboard provides a comprehensive overview of the status of devices, traffic distribution, and all the threats by the type for the users to prepare and respond to them when required. This also helps the users to improve the control over their cyber security measures.

The system dashboard NSM provides has four tabs: Devices, Summary, Network, and Threat.

The default view is Devices dashboard. It shows the summary of the devices and alerts in your infrastructure.

You can see the dashboard for any of the tenants, groups, or all tenants by clicking the tenant name at the top.



The **DEVICE** tab shows you a summary of your devices:

- **FIREWALLS**: Displays the number of firewalls that you intend to manage through NSM. Click FIREWALLS to list the firewalls in the Inventory page.
- **OFFLINE**: Displays the number of firewalls that are offline. Click OFFLINE to list the offline devices in the Inventory page.
- **EXPIRING LICENSES**: Displays the number of expiring licenses.
- **GROUPS**: Displays number of device groups. Click GROUPS to list the device groups.
- **USERS:** Displays the number of users online.

The **FIREWALL OVERVIEW** section shows how many devices are Online and Managed, Offline, Online and Unmanaged, Unassigned, and with Expired Licenses. A pie chart representation of firewall overview is also displayed. The geographical locations of the firewalls are shown on the map. For more details of the devices in a particular location, hover the mouse over the map location.

The **Alert Center** is shown at the bottom of the dashboard. You can also view the most recent alerts in the table below the summary. An alert summary is provided and you can click on any of the categories—All, Threats, or General to view the Notification Center and see all the alerts for the selected category.

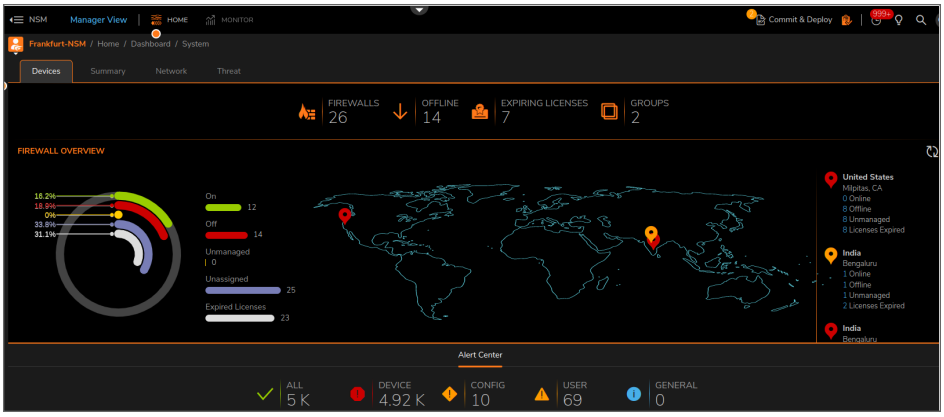
The **Summary** tab shows Traffic Distribution, Top Users, Observed Threats, and Top Devices by Sessions in your network infrastructure for the period selected in the slider at the top. It also shows the Insights section giving information about the number of infected hosts and the number of critical attacks. You can drill down further by selecting the Date or Alphabetical order options. You can also filter the data with **View Details** link.

The **Network** tab shows data pertaining to transactions in your network infrastructure. This include the details of top applications, addresses, users, and the top web categories from which connections are initiated. Each space enables you to filter the data with available options. You can also drill down further by clicking on the **View Details** link.

The **Threat** tab shows the details of threats by type including the top viruses, intrusions, spyware, and botnet. You can drill down further by clicking on the **View Details** link.

MONITOR Features

When you click **MONITOR** in **MANAGER VIEW**, it takes you to reporting features.



The **MONITOR** feature for NSM Essential firewalls create **Summary** and **Details** reports based on the following:

- **Applications**
- **Users**
- **Viruses**
- **Intrusions**
- **Spyware**
- **Web Categories**
- **Addresses**
- **Locations**

Use the slider at the top to get report for a specific time period. Your options are from 15 minutes to 7 days. Hover over the chart to get detail for any specific point of time.

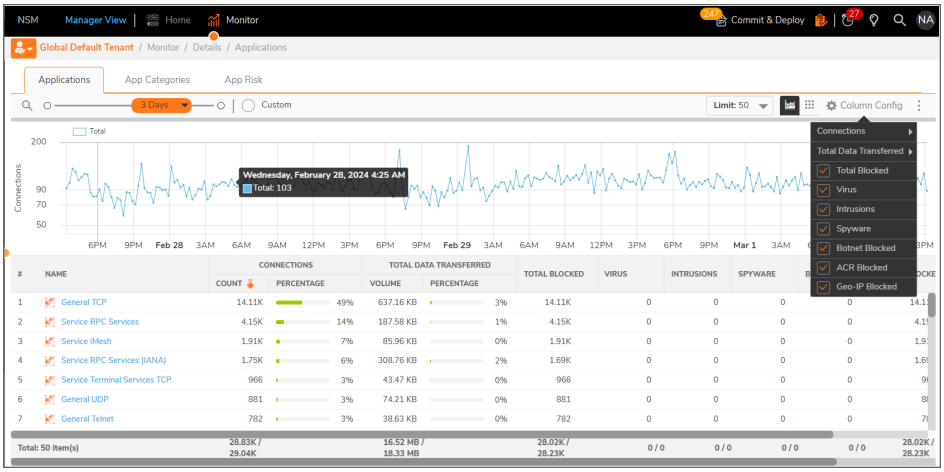
In case of NSM Advance firewalls, the slider will have option from 1 hour to 365 days.

To export report data:

1. Click **Export** option on top of the chart.
2. Select one of the options: Generate Flow Report PDF (Disabled in **MANAGER VIEW**), Download Capture Threat Assessment, and Export Grid Data as CSV.

ⓘ | **NOTE:** The maximum rows allowed in the report are 8K.

You can further drill down on this Chart & Grid report based on Connections, Total Data Transferred, Total Blocked, Virus, Intrusions, Spyware, Botnet Blocked, ACR Blocked and Geo-IP Blocked. These options change based on the type of report selected.



3

Group and Tenant Reporting

Group and Tenant reporting offers you additional ways in which to combine or filter data so you can lean more about the activity in your network environment. These reports aggregate data from all the firewalls in a particular group or a tenant which helps an administrator get visibility in network activities within that group or tenant. The level of reporting depends upon the type of NSM license you bought. Firewalls with an Essential license provide different reporting and analytical capabilities than those with an Advanced license. In cases of tenants and groups having firewalls with mix of Essential and Advanced licenses, report data is aggregated based on each license type.

The data here provides an overview so you understand how the interface and the drill-down options are arranged. Depending on the problem you are trying to solve or the symptoms your are trying to resolve, you can research the problem in several different ways. Since one environment is somewhat different from another, the key to making the best use of the Group and Tenant reporting is to explore the different reports and reporting views on your own. Familiarity with how to navigate the options makes it easier for you to navigate when you need to search for answers.

Topics:

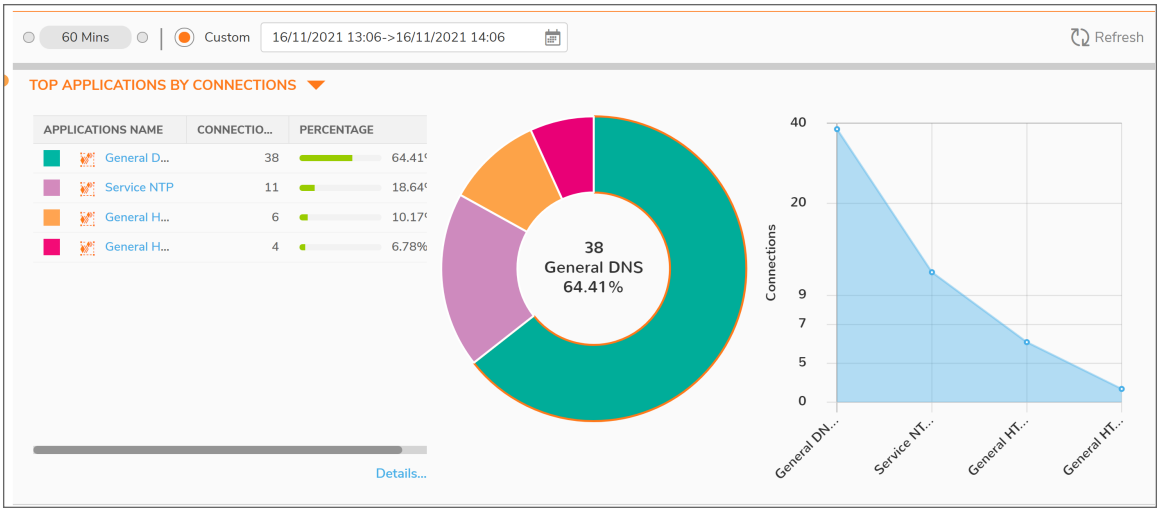
- Understanding How the NSM License Affects Reporting
- Navigating Reports
- Tenant Reports
- Group Reports
- Custom Reports

Understanding How the NSM License Affects Reporting

The type of licensing you have affects the reports and analytics options you have available to you.

When You Have a Firewall Essential License

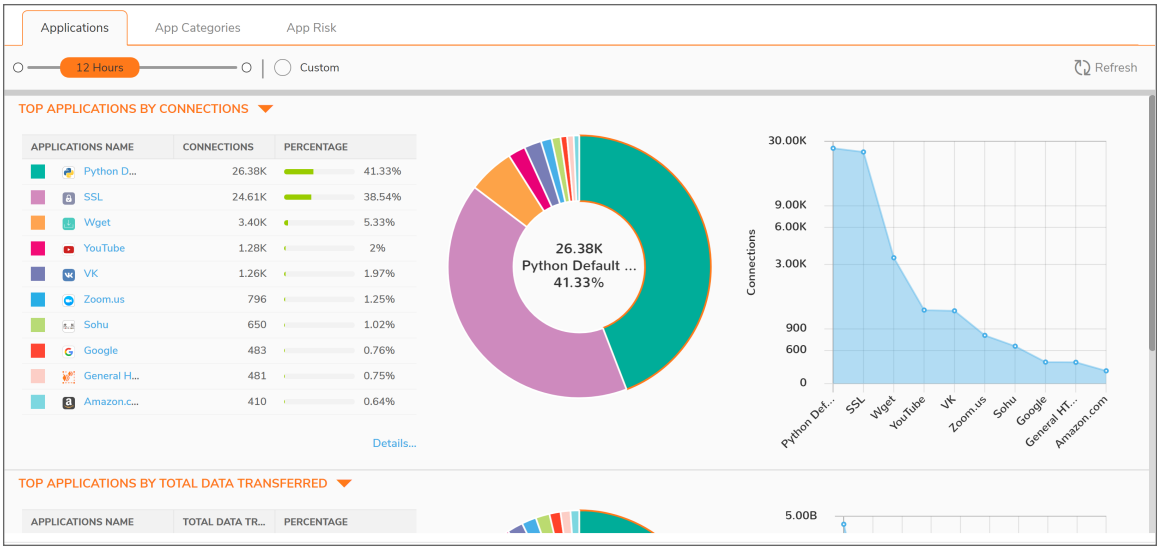
When you have a firewall with an Essential license, only the most basic reporting coverage is provided.



Reporting is limited to a small set of **Summary** reports and the matching **Details** reports. With the Essential license, you don't have the ability to drill down from a tenant or group view of the data, nor do you have access to all the reporting and analytics options. To see details on a specific firewall you need to navigate to **Firewall View** and then select **Monitor**.

When You Have a Firewall Advanced License

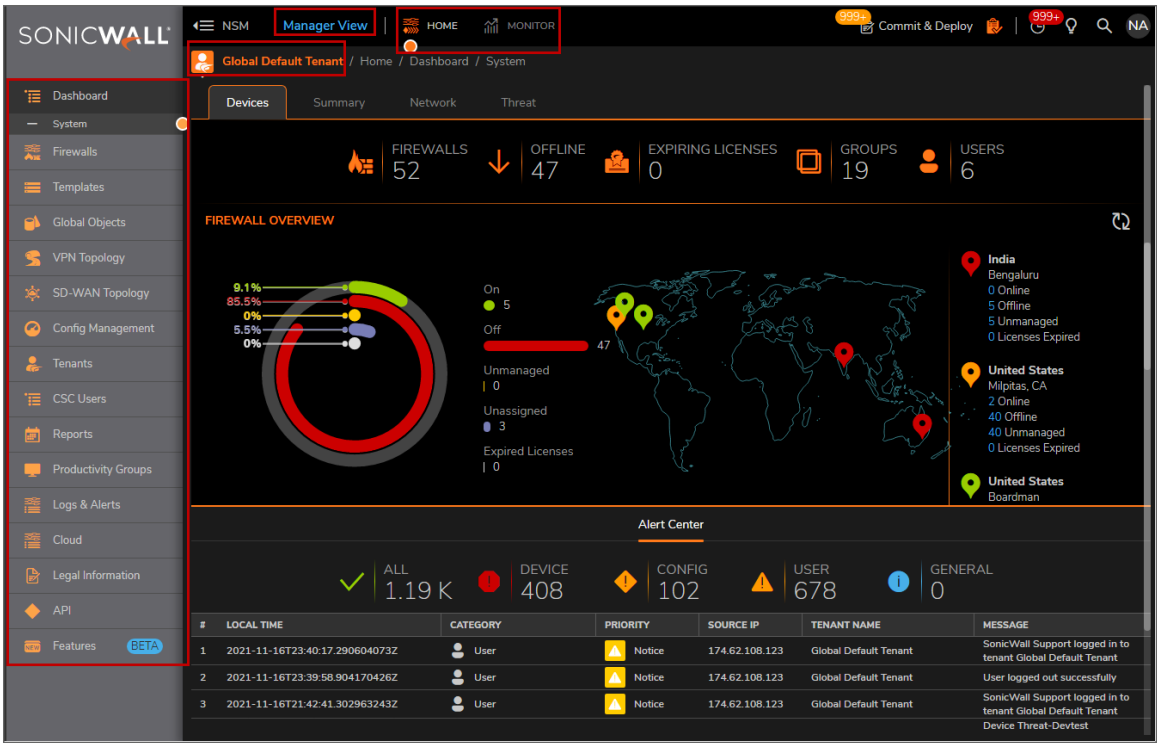
The Advanced license provides additional coverage: You have access to many more reports and drill-down capability to log sessions. You also have different views of the information. Tenant reports let you see the amalgamation of a tenant's devices in a single view. Group reports are also available. You can see data combined, based on a group that you set up.



Navigating Reports

When you first log into an NSM instance, you are taken to the main Dashboard screen. The Dashboard might also be the first place you see an indicator of an issue. A few key things to remember about the Dashboard and navigation in general.

- The default view is the **Manager View**.
- The default option at the top is the **Home** option.
- The default command option is **Dashboard > System**, showing the Devices tab.



You can think of this as your starting place. Changing any one of these selections offers access to different data. Become familiar with the layout of these options so you can easily change them when navigating issues.

The next most important option is the **Monitor** option (next to **Home** or on a list that drops down after clicking on **Home**). You can select **Monitor** to see reporting based on a selected tenant or a group.

Tenant Reports

Tenant reports trigger off the selected tenant. A particular tenant report aggregates the data from all the firewalls that make up that tenancy.

To navigate to the tenant reports:

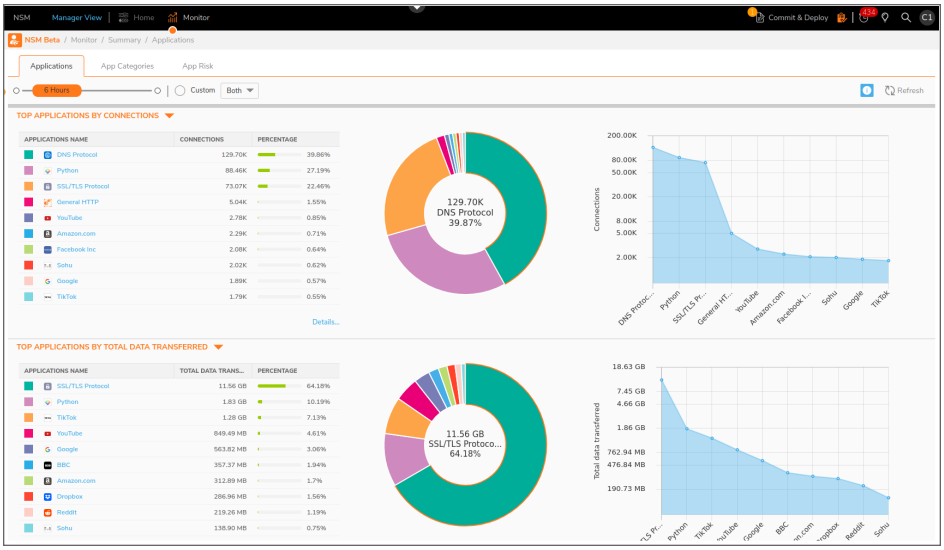
1. Click the tenant name at the top and select the tenant you want to see reporting for. If you have a long list of tenants, you can type a string in the search field to filter the list.
2. Select the **Monitor** option at the top.

Summary Reports

The reports displayed shows an amalgamation of the data based on the devices that make up that tenant's infrastructure. The **Summary** reports summarize the information for the topics listed.

- **Duration** : Use the slider to choose the report time duration in hours or days. The **Custom** option lets you to choose a specific duration from the calendar.
- **Refresh**: Refreshes the data on the page.
- **Chart Titles**: Use the drop-down list in the chart title to select which the charts you want to display.

The following is an example of the **Applications** Summary. Note that some reports like the **Applications** Summary have additional tabs with more data.



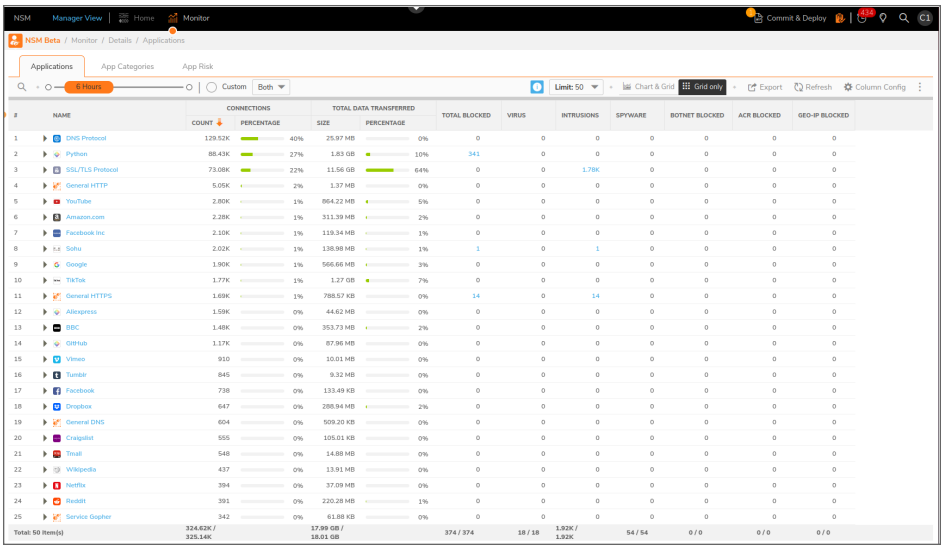
Run your mouse over the graphs. As it runs over an option in the chart or a data point in the graph, additional details pop up about that data. Some of the tables also have links in them that lead to more data. For example,

click on one of the application names to get a full description. Click on the **Details...** link to jump to the matching **Details** report.

Detail Reports

When viewing the **Details** reports, you have additional options to customize the data.

- **Duration** : Use the slider to choose the report time duration in hours or days. The **Custom** option lets you to choose a specific duration from the calendar.
- **Limit**: Allows you to set how many items appear on a page. Options range from 10 to 8000.
- **View by Chart or List**:Click the appropriate icon to view the information in a chart and grid (list) or in a grid only.
- **Export**: Allows you to export the grid data to a CSV file.
- **Refresh**: Refreshes the data on the page.
- **Column Config**: Check the desired boxes that you want to display in the table.
- **More Options**:Choose **More Options** to navigate to **Home > Reports > Rules** or **Home > Reports > Saved Reports** set up reports and access saved reports.



ⓘ | **NOTE: Graph View** is not supported at the Tenant and Group level.

On the Details page you can drill down in different ways to get more information. Clicking the arrow by the element name expands the description and shows how the aggregated data that is spread across firewalls. Any of the data represented in blue is an active link. Click on it to show the details. Some values also link to other reports. For example, click on one of the **Total Blocked** values and jump to the **Session Logs**. The Session Logs has more links you can click on for additional detail.

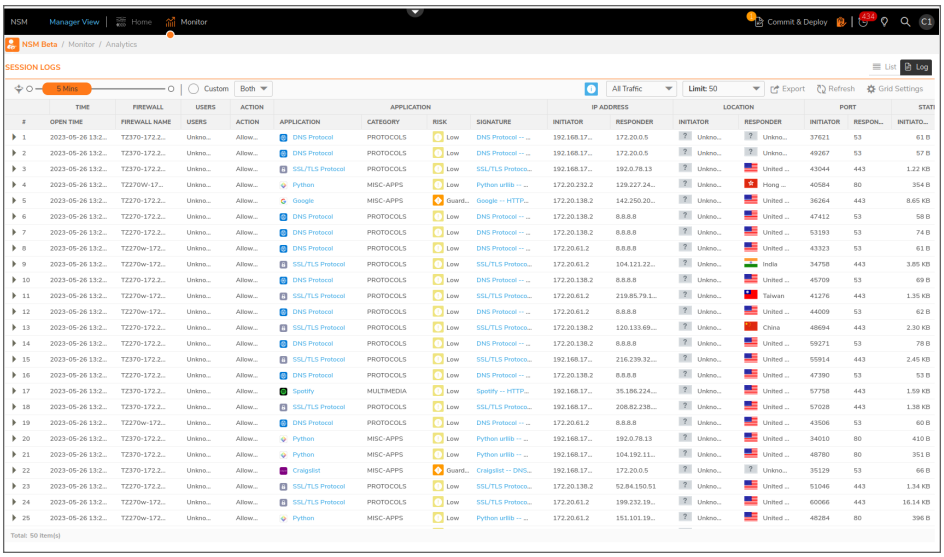
ⓘ | **NOTE:** The drill-down to session logs, or Analytics, is not available for firewalls with the Essential License.

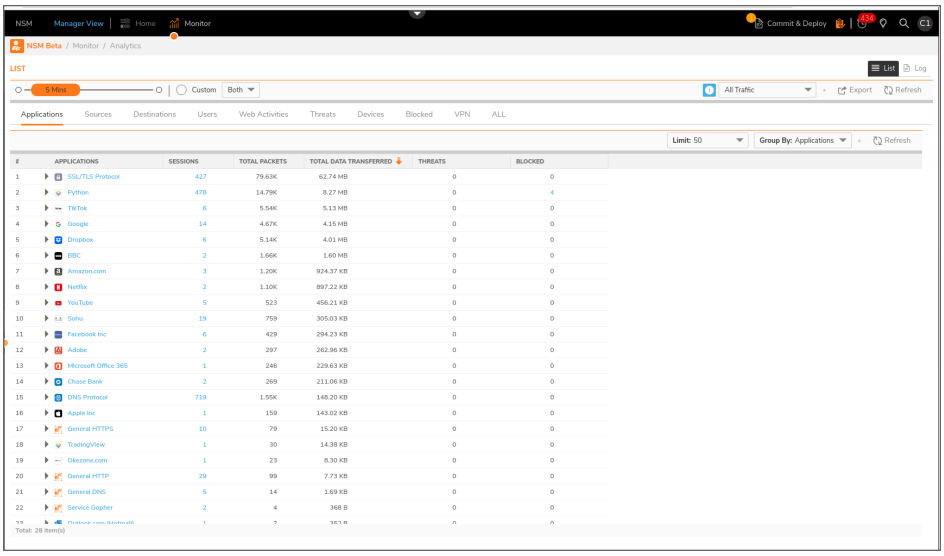
Tenant Analytics

Tenant analytics aggregates the session logs from all the firewalls that make up that tenancy. Analytics is only available if the tenant has firewalls with the Advanced License.

To navigate to the tenant analytics:

1. Click the tenant name at the top and select the tenant you want to see Analytics for. If you have a long list of tenants, you can type a string in the search field to filter the list.
2. Select **Monitor > Analytics**.





The display shows an amalgamation of the session logs on the devices that make up that tenant's infrastructure. You can customize how the analytics report appears.

- **Duration** : Use the slider to choose the report time duration in hours or days. The **Custom** option lets you to choose a specific duration from the calendar.
- **Traffic types**: Click a drop-down menu and select the type of logs you want to display. Options include **All Traffic**, **Web Activities**, **Threats**, or **Blocked**.
- **Limit**: Allows you to set how many items appear on a page. Options range from 10 to 8000.
- **Export**: Allows you to export the grid data to a CSV file.
- **Refresh**: Refreshes the data on the page.
- **Grid Settings**: Allows you to show or hide specific fields of the session logs.
- **List/Log**:Choose **List** or **Log** to set the style of the display.

Within the logs, the fields highlighted in blue are active links. Click on the link to see more detail.

Group Reports

Group reports trigger off the group selected. A group report aggregates the data from all the firewalls that make up that group.

To navigate to the group reports:

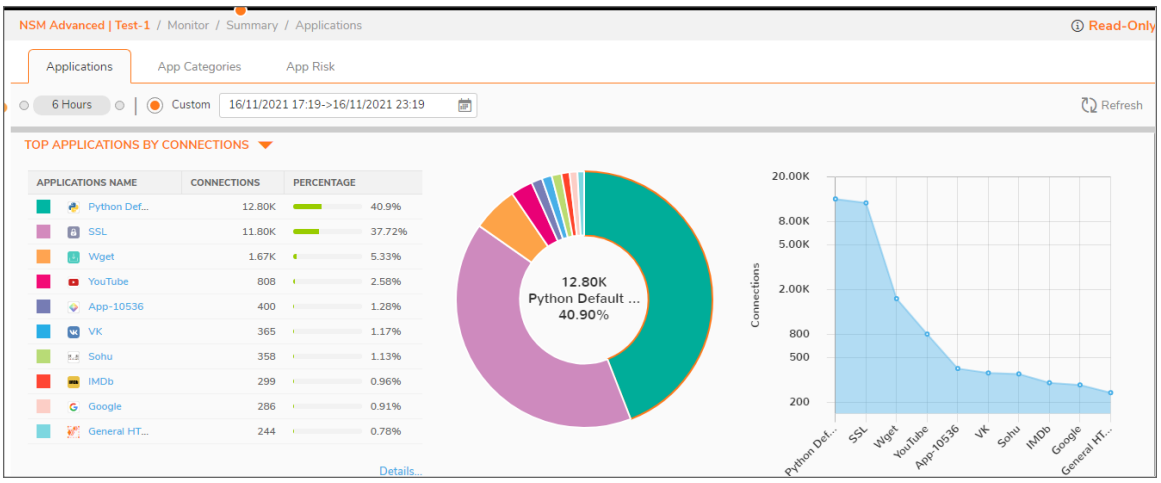
1. On the **Manager View** select **Home > Firewalls > Groups**.
2. Select the group you want to see the reports for.
3. Select the **Monitor** option at the top.

Summary Reports

The reports displayed shows an amalgamation of the data based on the devices that make up that groups's infrastructure. The **Summary** reports summarize the information for the topics listed.

- **Duration** : Use the slider to choose the report time duration in hours or days. The **Custom** option lets you to choose a specific duration from the calendar.
- **Refresh**: Refreshes the data on the page.
- **Chart Titles**: Use the drop-down list in the chart title to select which the charts you want to display.

The following is an example of the **Applications** Summary. Note that some reports like the **Applications** Summary have additional tabs with more data.

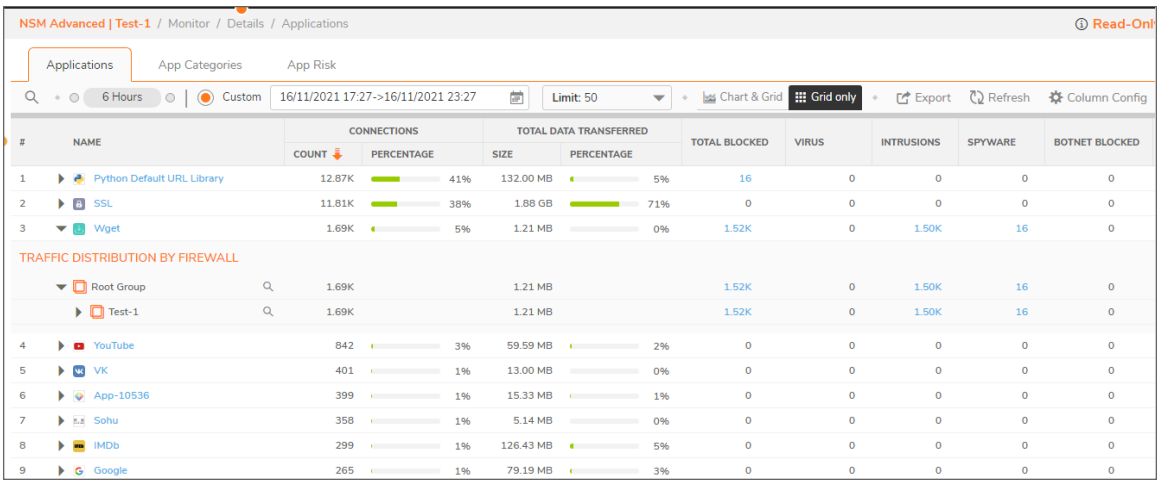


Run your mouse over the graphs. As it runs over an option in the chart or a data point in the graph, additional details pop up about that data. Some of the tables also have links in them that lead to more data. For example, click on one of the application names to get a full description. Click on the **Details...** link to jump to the matching **Details** report.

Detail Reports

When viewing the **Details** reports, you have additional options to customize the data.

- **Duration** : Use the slider to choose the report time duration in hours or days. The **Custom** option lets you to choose a specific duration from the calendar.
- **Limit**: Allows you to set how many items appear on a page. Options range from 10 to 8000.
- **View by Chart or Grid**:Click the appropriate icon to view the information in a chart and grid (list) or in a grid only.
- **Export**: Allows you to export the grid data to a CSV file.
- **Refresh**: Refreshes the data on the page.
- **Column Config**: Check the desired boxes that you want to display in the table.



On the Details page you can drill down in different ways to get more information. Clicking the arrow by the element name expands the description and shows how the aggregated data that is spread across firewalls. Any of the data represented in blue is an active link. Click on it to show the details. Some values also link to other reports. For example, click on one of the **Total Blocked** values and jump to the **Session Logs**. The Session Logs has more links you can click on for additional detail.

ⓘ | **NOTE:** The drill-down to session logs, or Analytics, is not available for firewalls with the Essential License.

Group Analytics

Group analytics aggregates the session logs from all the firewalls that make up that group. Analytics is only available if the group has firewalls with the Advanced License.

To navigate to the tenant analytics:

1. On the **Manager View** select **Home > Firewalls > Groups**.
2. Select the group you want to see the reports for.
3. Select the **Monitor > Analytics**.

The display shows an amalgamation of the session logs on the devices that make up that group's infrastructure. You can customize how the analytics report appears.

- **Duration** : Use the slider to choose the report time duration in hours or days. The **Custom** option lets you to choose a specific duration from the calendar.
- **Traffic types**: Click a drop-down menu and select the type of logs you want to display. Options include **All Traffic**, **Web Activities**, **Threats**, or **Blocked**.
- **Limit**: Allows you to set how many items appear on a page. Options range from 10 to 8000.
- **Export**: Allows you to export the grid data to a CSV file.
- **Refresh**: Refreshes the data on the page.

- **Grid Settings**: Allows you to show or hide specific fields of the session logs.
- **List/Log**:Choose **List** or **Log** to set the style of the display.

Within the logs, the fields highlighted in blue are active links. Click on the link to see more detail.

4

Firewall View

This section describes the features available in the Firewall View.

- Live Monitoring, Live Report and Up Time Report
- Reports and Analytics
- NSM - Advanced
- VPN Reports

Live Monitoring, Live Report and Up Time Report

Live monitoring, live reporting and up time reporting features are organized under **Overview**. Live Monitor charts can be used to monitor Applications, Bandwidth Usage, Connection Usage, CPU/Memory Usage, and Per Interface Usage.

Live Monitor

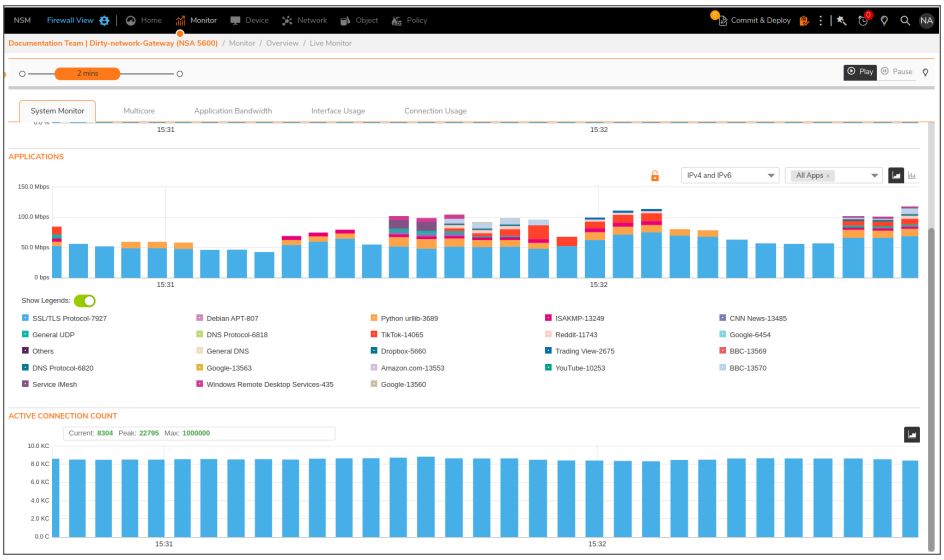
Live Monitor provides a real-time view of the packets forwarded by the firewall and is visible when viewing from individual firewalls. When you select Group View or Global View in the Device Manager, the Live Monitor option is not shown. The Live Monitor is always running, but it shows only the current data. A background task is saving the data to a database. All data shown in Live Monitor is saved for historical reasons and you can find it in Live Reports.

The following reports are shown in Live Monitor:

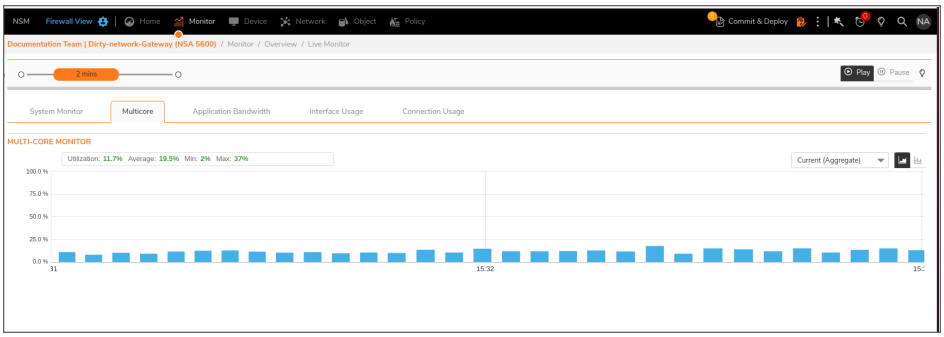
- **System Monitor**
- **Multi-Core Monitor**
- **Application Bandwidth**
- **Interface Usage**
- **Connection Usage**

NOTE: You can filter the information on the **Application Bandwidth** and the **Interface Usage** tabs according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

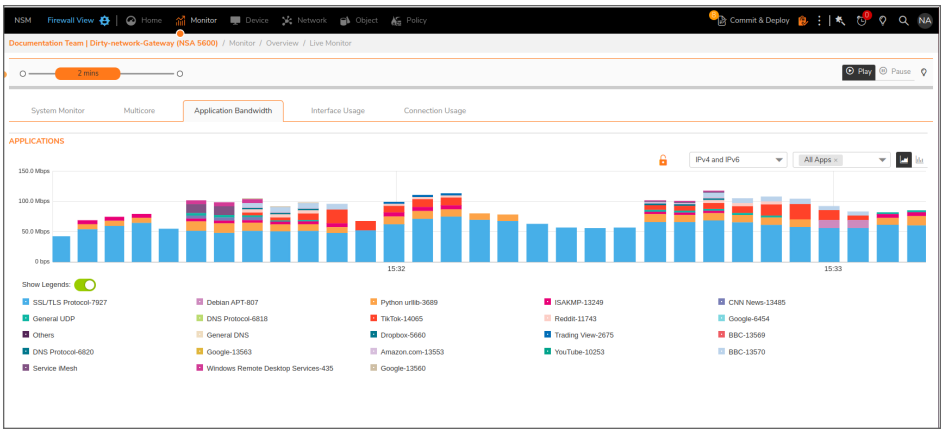
System Monitor



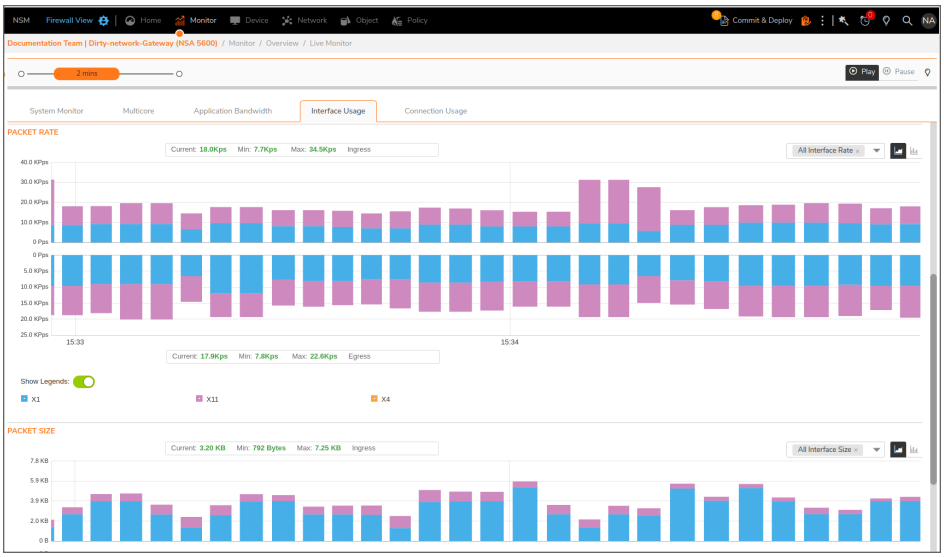
Multi-Core Monitor



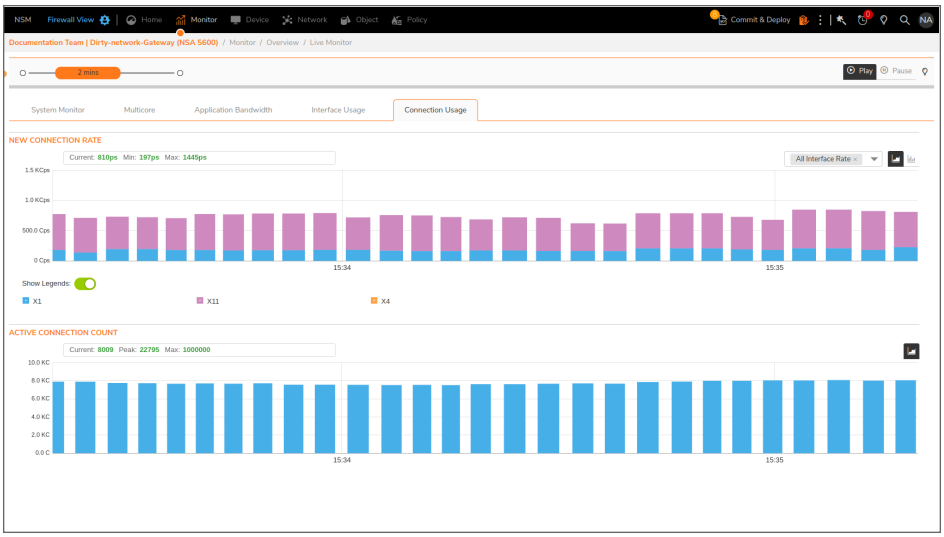
Application Bandwidth



Interface Usage



Connection Usage



Live Report

Live Report provides historical Live Monitor data. You can get Live Report for a specific time by adjusting the slider or entering a custom time. You can choose and visualize a real-time chart of any stored historic time data.

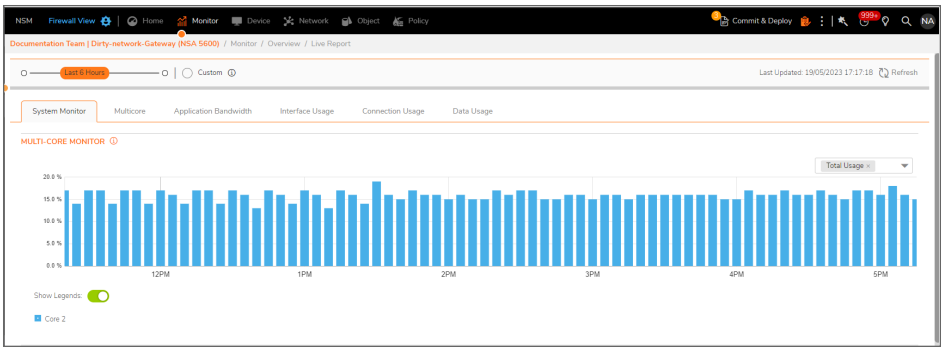
Mouse over a data point to see values at that instant. Select Start Time and End Time in the chart and click Refresh icon to get drill-down data for that particular time.

The following reports are shown in Live Report:

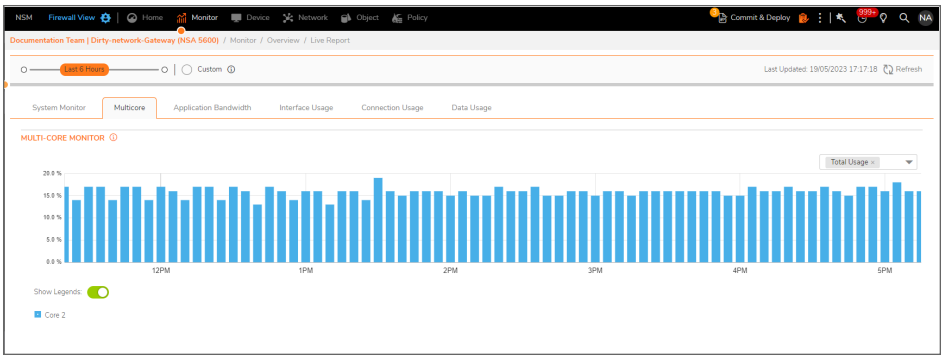
- **System**
- **Multi-Core**
- **Application Bandwidth**
- **Interface Usage**
- **Connection Usage**
- **Data Usage**

ⓘ **NOTE:** You can filter the information on the **Application Bandwidth** and the **Interface Usage** tabs according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

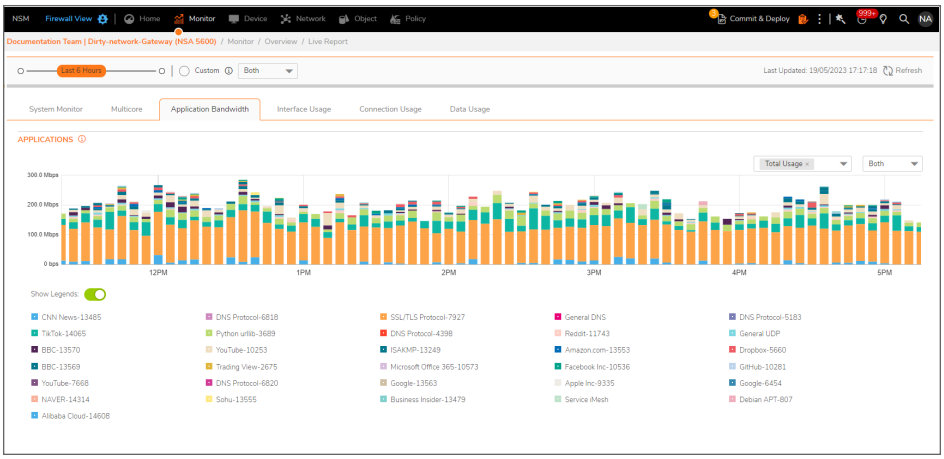
System



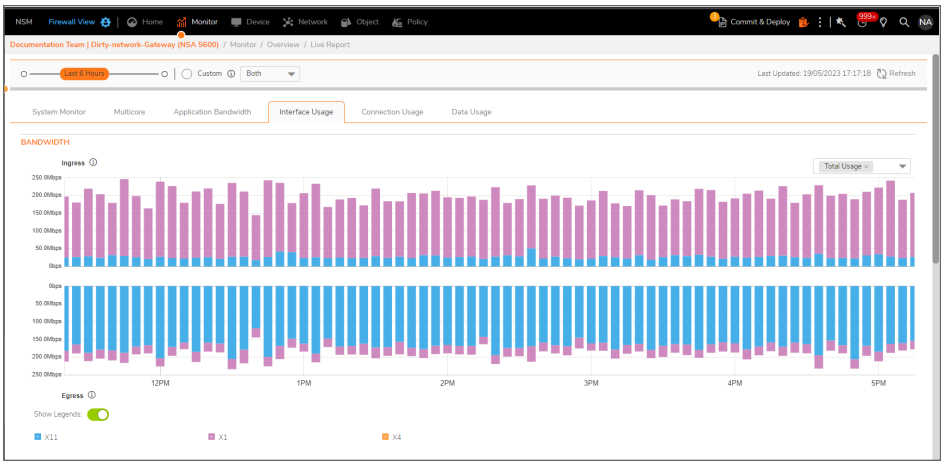
Multi-Core



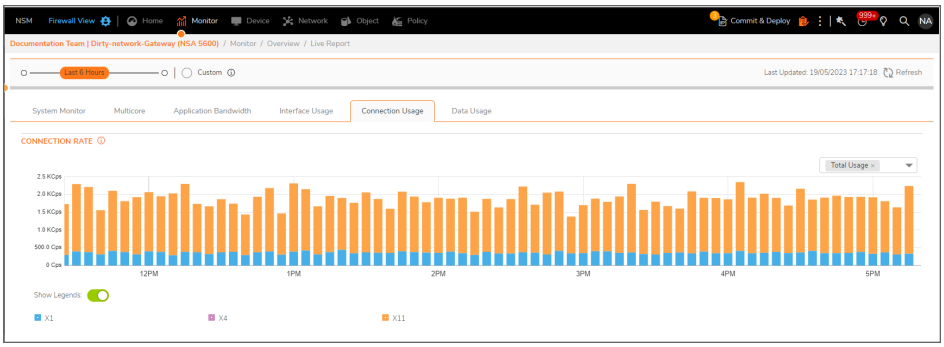
Application Bandwidth



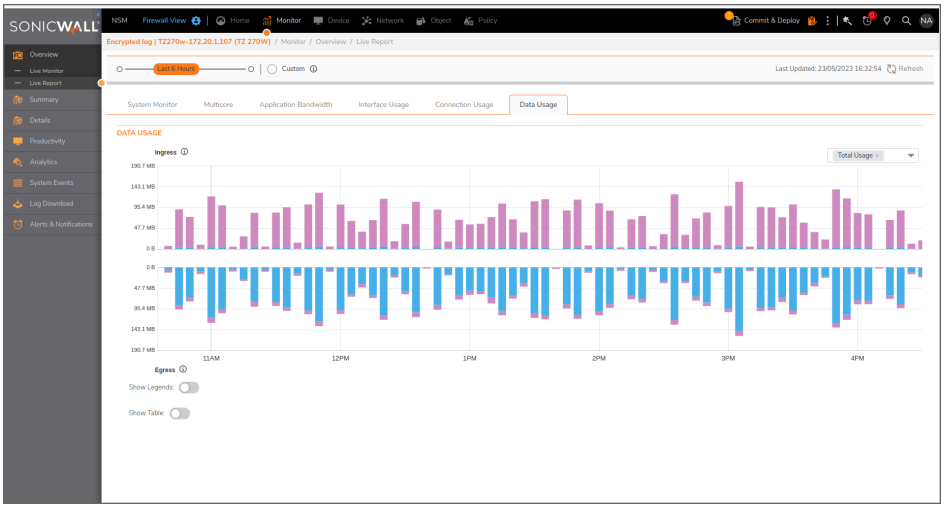
Interface Usage



Connection Usage



Data Usage



ⓘ **NOTE:** Data Usage is available from NSM SaaS **2.3.5** onwards for both **GEN6** and **GEN 7** firewalls. You can refer the Release Notes to learn more about the build information.

ⓘ | **NOTE:** Data Usage report requires the flow log transport mechanism to be changed to encrypted mode.

Up Time Report

Up Time Report a real-time view of the up time and down time information of the firewall. The data can be viewed in graph as well as grid view.

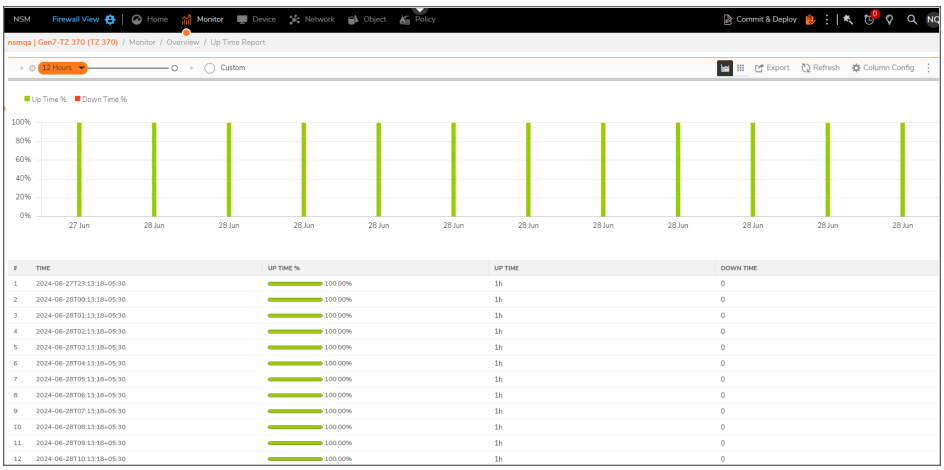
You can use the **Time Slider** to adjust the time duration and the **Custom** button to customize the dates. The slider allows you to view the report from a duration of 12 hours to 30 days. If you select a time range of 12 or 24 hours, then the report will be shown in the interval of 1 hour. If you select a time range of 3, 5, 7 or 30 days, then the then the report will be shown in the interval of 24 hours.

You can also export the data in CSV and PDF formats using the **Export** button and refresh the page using the **Refresh** button. The **Column Config** button allows you to check the desired boxes that you want to display in the table.

ⓘ | **NOTE:** The Up Time Report is available for both **NSM Advanced** and **NSM Essential** License.

ⓘ | **NOTE:** The Up Time Report is available for **Gen7** firewalls.

ⓘ | **NOTE:** The Up Time Report is available at **tenant, group and firewall** level.



Reports and Analytics

The Summary reports provide various types of data being tracked for your security infrastructure. Think of these as executive summary reports that you can start with to check the general health for the topics listed. If an issue is reported, you can drill down from them.

At the top of the summary reports—no matter what topic you pick, you can customize and manage the reports displayed.

Option	Description

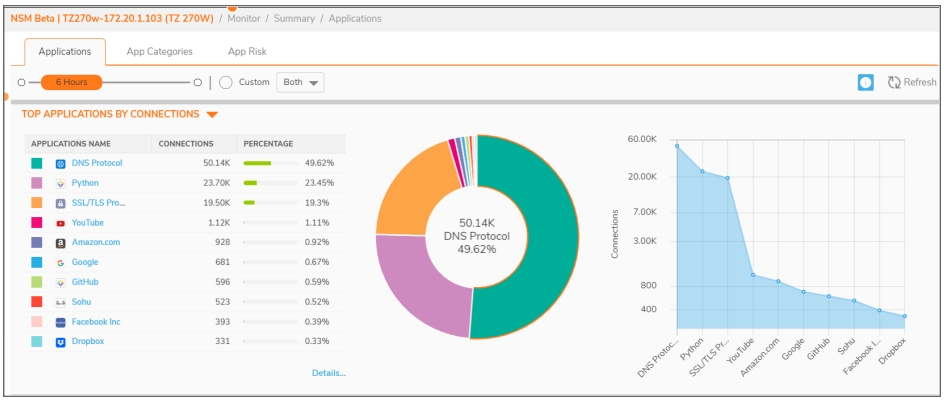
Sliding bar	Slide left or right to select a predefined period for the reports to cover. The range is 1 hour to 365 days.
Custom option	Define a custom period for the reports to cover. Select starting and ending dates and times for the custom period.
By	Filter data by any one of the parameters.
Limit	Number of connections.
Export	Provides three options: • Generate Flow Report PDF: Generates a PDF document of the flow reports being displayed. The file is stored at Scheduled Reports | Archive. The report may take several minutes to generate. • Download Capture Threat Assessment: opens as an html file. • Export Grid Data as CSV: Downloads as a csv file.
Refresh	Refreshes to the latest data.
Column Config	Add or remove categories as columns in the table.
Vertical Ellipses icon	Provides two options: • Go to PDF Rules: Takes you to **Scheduled Reports** > **Rules**. • Go to PDF Archives: Takes you to **Scheduled Reports** > **Archive**.

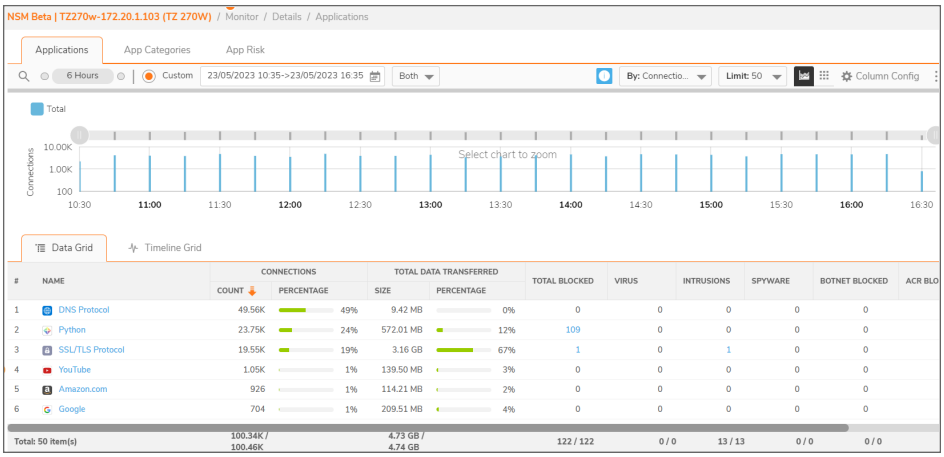
NSM - Advanced

This section provides the options that are listed under NSM - Advanced screen. This screen is available for NSM Advance license where you can view the Tenant and Group level reporting. Click on **Details**, below each report, to go to the details page of the report .

Applications

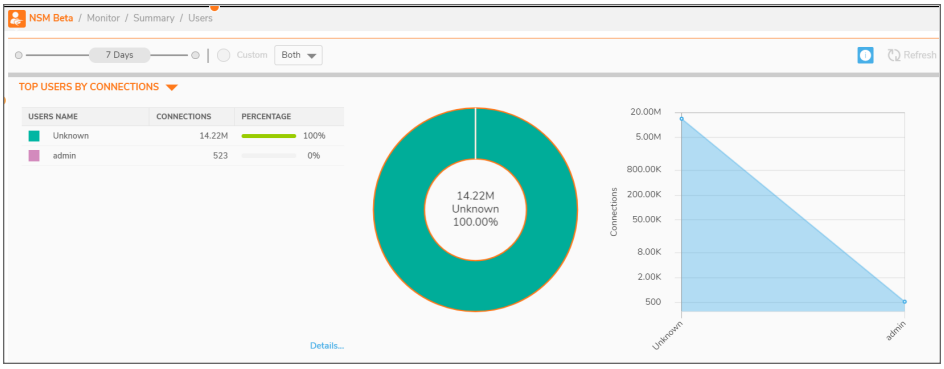
The Applications summary page has three types of reports displayed by default: Applications, App Categories, and App Risks.

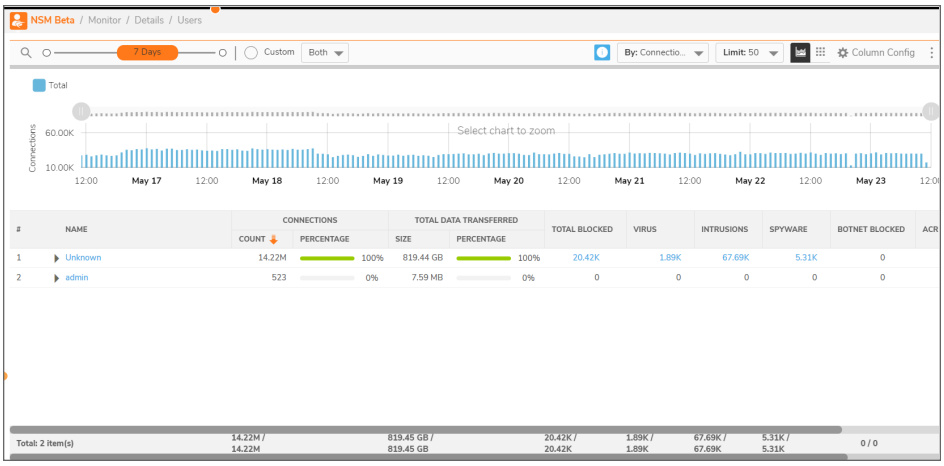




Users

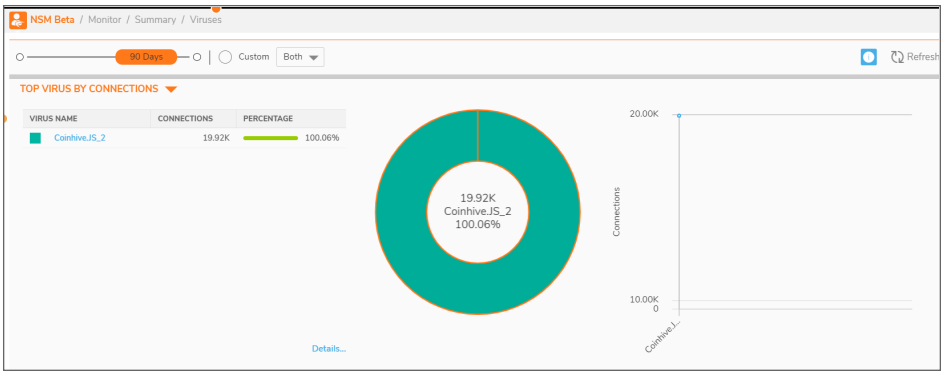
This report provides data that relates to the users connected to the system. You can track user level transactions and activities by filtering on different drill-down options.

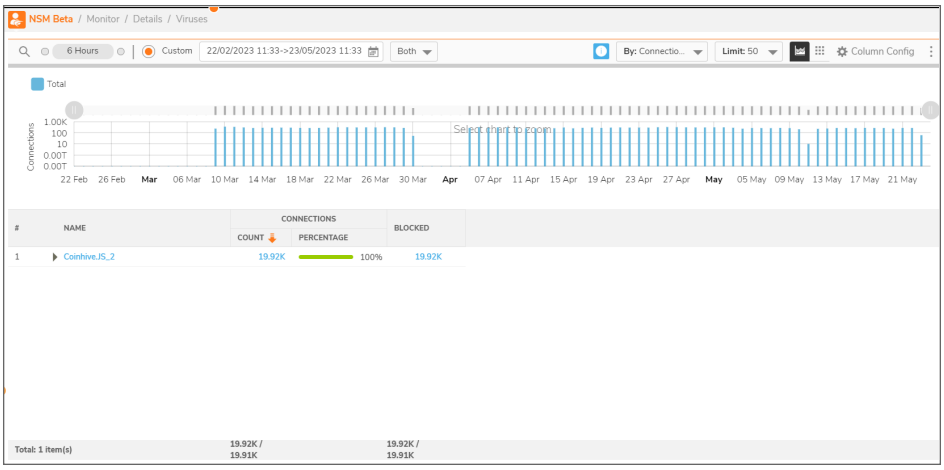




Viruses

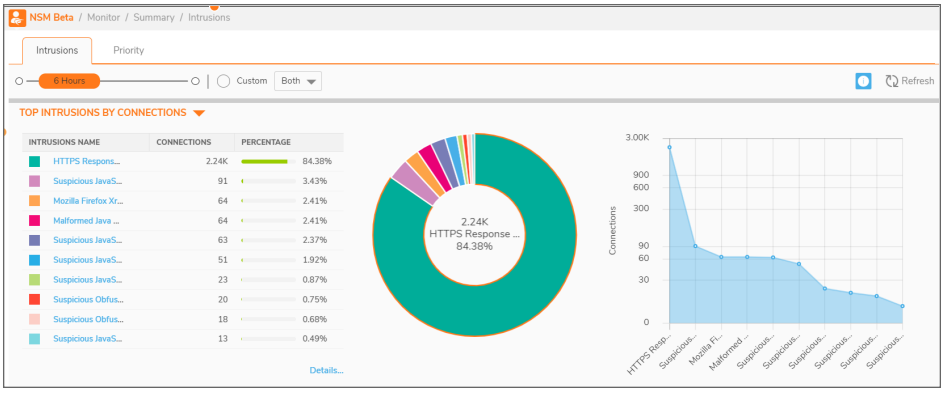
This report tracks the viruses that have been detected. You can filter on connections they occurred on or by which viruses were blocked. Details are provided in the table. Click on **HOME > Summary > OBSERVED THREATS** to see the reports on virus, botnet, spyware, and intrusion.

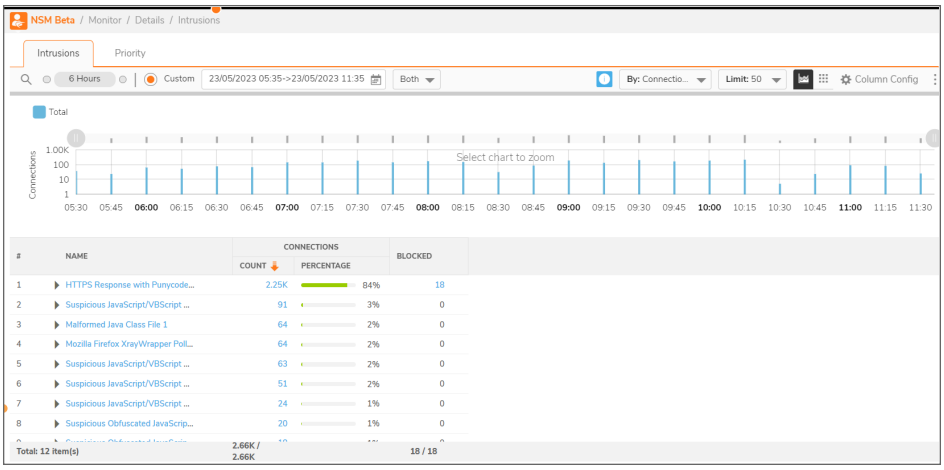




Intrusions

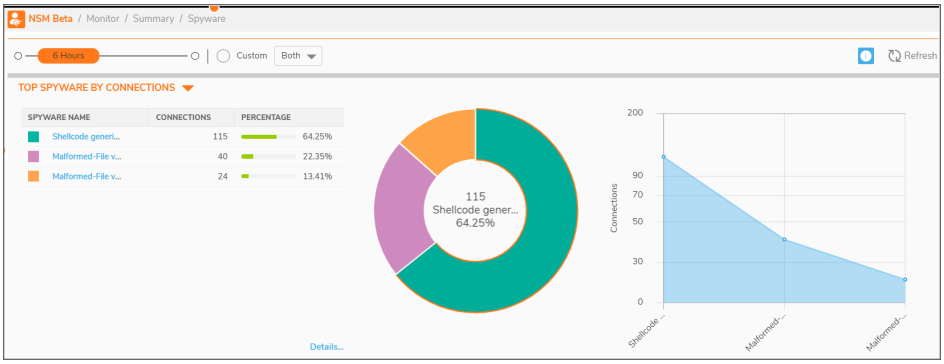
The Intrusions summary has two types of reports (represented by the different tabs): **Intrusions** and **Priority**. The Intrusions report tracks the disturbances that have been detected. You can filter on connections that occurred on or by which intrusions were blocked. Details are provided in the table.

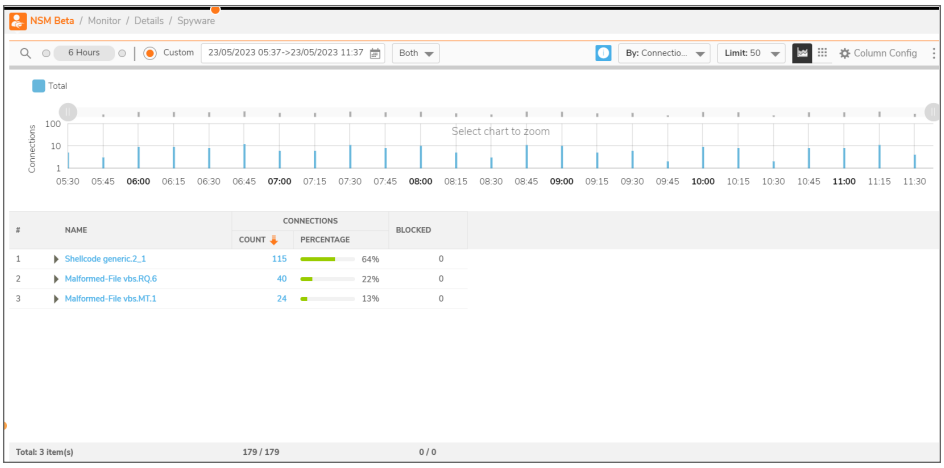




Spyware

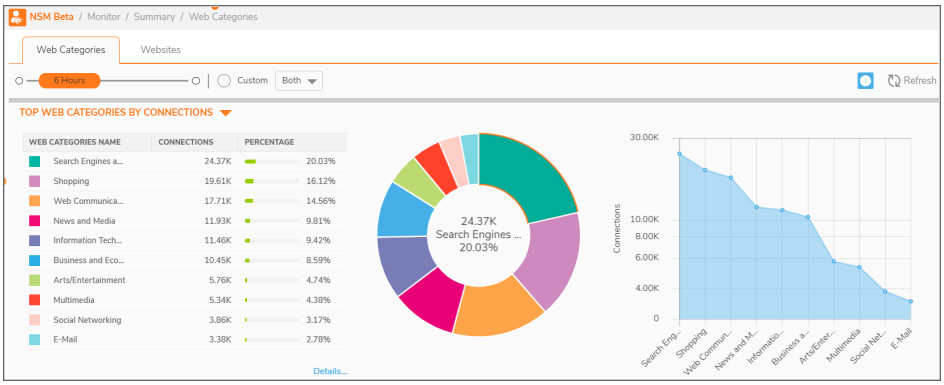
This report tracks the spyware that has been detected. You can filter on connections they occurred on or by which spyware was blocked. Two summary reports are available and displayed by default: Spyware by Connections and Spyware by Blocked.

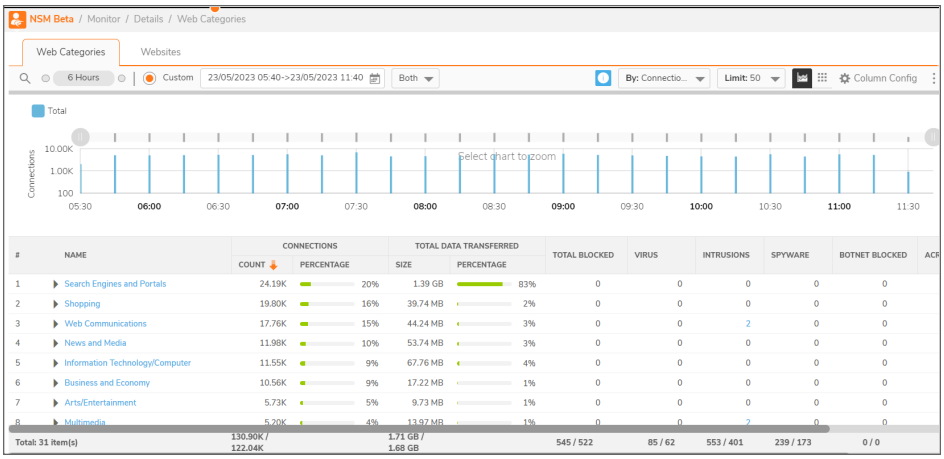




Web Categories

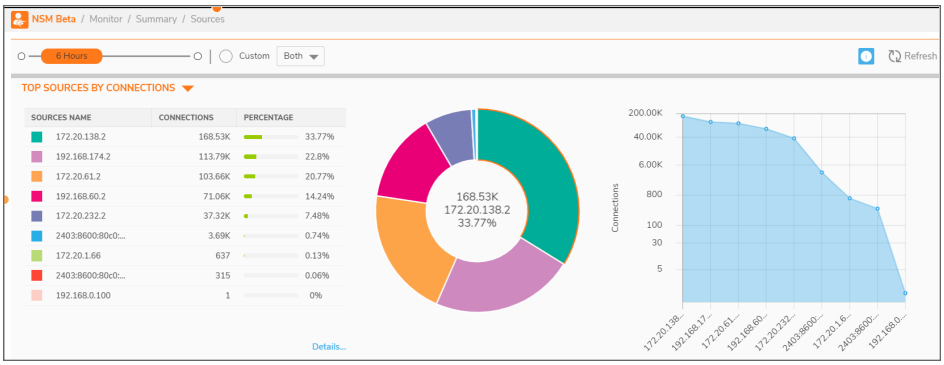
On the NSM system, the Web Categories summary has two types of reports. **Web Categories** and **Websites**. This report displays the number of connections based on web categories. You can filter on the categories in the View drop-down list. Details are provided in the table. Click on **HOME > Network > Web Categories** to see the web categories report. Two summary reports are available and displayed by default: Web Categories by Connections and Web Categories by Total Data Transferred.





Sources

This report displays the number of connections based on IP address of the source. You can filter on the source type listed in the drop-down list. You can also find the data in the form of a Pie Chart as well as a Graph

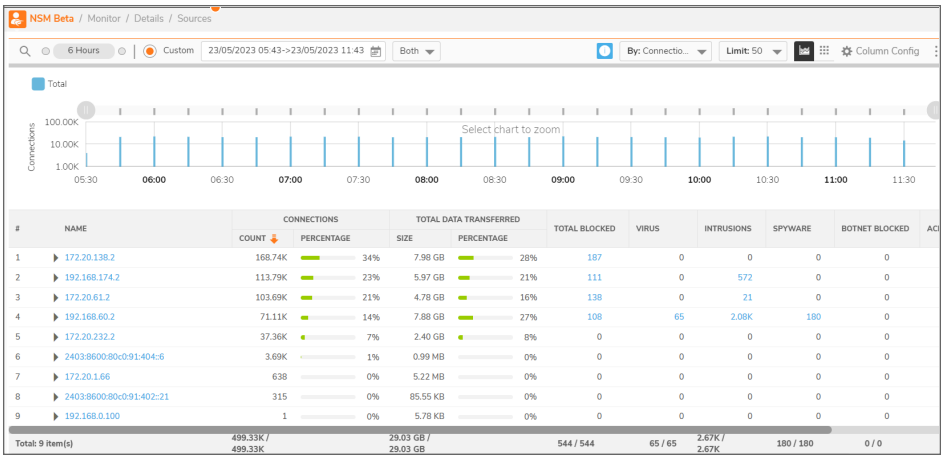


Click on **Details**, below each report, to go to the details page of the Source report. You can also view the page by navigating to **Details > Sources**. The top of the **Details** page shows a graphical representation of the selected **By Metric** data over a time period.

The bottom of the page has a table that shows information such as name of the source IP addresses, connections and total data transferred. The rest of the columns of the table can be selected from the **Column Config** button at the top of the page. The total information of each column can be seen at the extreme bottom of the page.

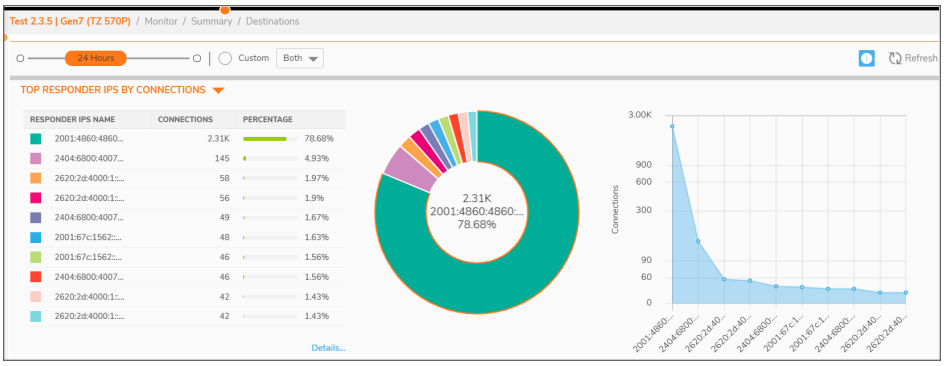
You can filter the information according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

The **Search** button at the top of the page allows you to search multiple IP adresses at the same time using the **CIDR** method. For example, you can search 142.250.0.0/16 to see all the subnets under the series 142.250. You can also search 142.250.196.0/24 to see all the subnets under the series 142.250.196.



Destinations

This report displays the number of connections based on IP address of the destination. You can filter on the destination type listed in the drop-down list. You can also find the data in the form of a Pie Chart as well as a Graph

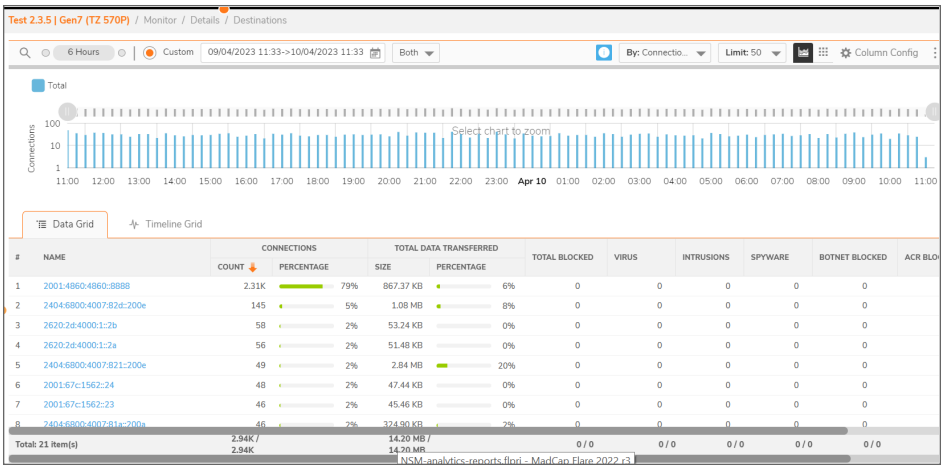


Click on **Details**, below each report, to go to the details page of the Destination report. You can also view the page by navigating to **Details > Destinations**. The top of the **Details** page shows a graphical representation of the selected **By Metric** data over a time period.

The bottom of the page has a table that shows information such as name of the destination IP addresses, connections and total data transferred. The rest of the columns of the table can be selected from the **Column Config** button at the top of the page. The total information of each column can be seen at the extreme bottom of the page.

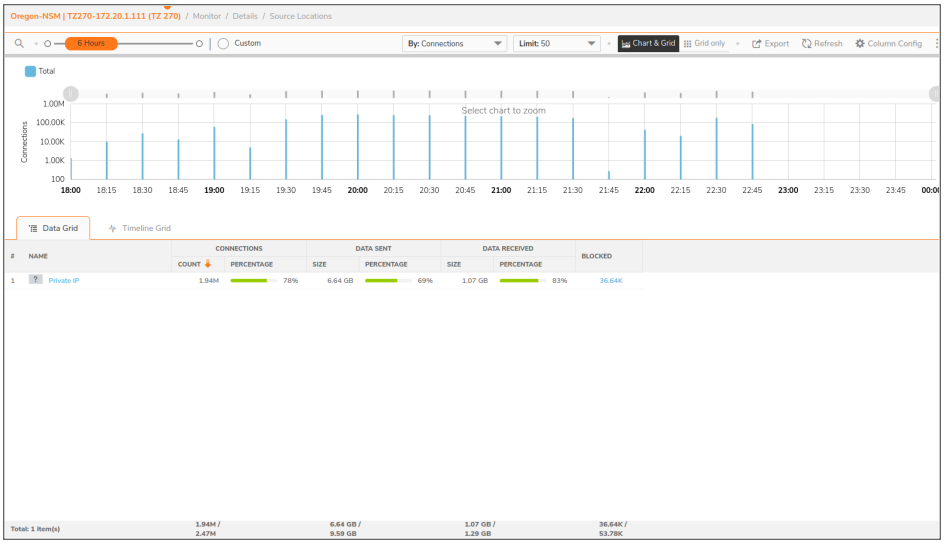
You can filter the information according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

The **Search** button at the top of the page allows you to search multiple IP adresses at the same time using the **CIDR** method. For example, you can search 142.250.0.0/16 to see all the subnets under the series 142.250. You can also search 142.250.196.0/24 to see all the subnets under the series 142.250.196.



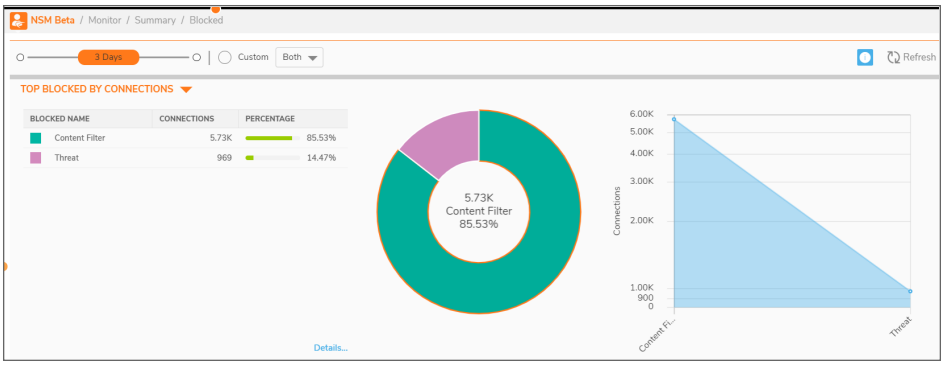
Locations

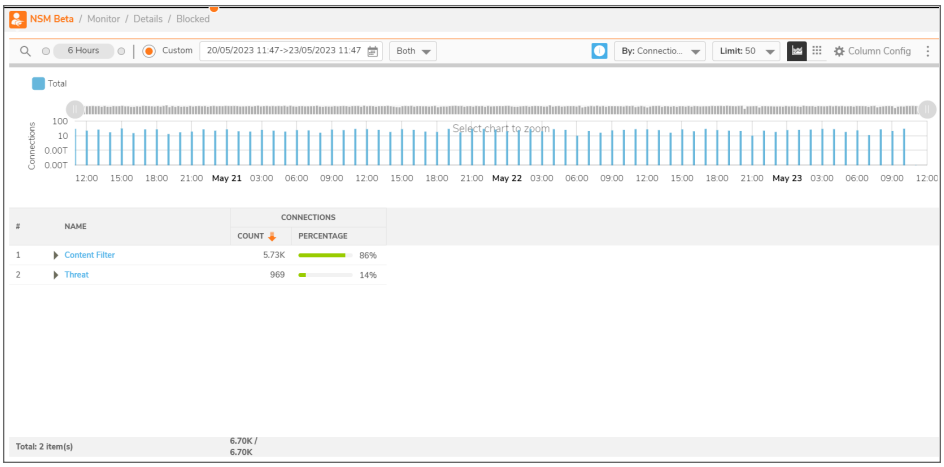
This report displays the top locations by connections and the top locations by total data transferred. The detailed summary includes the list of connections, total data transferred, data sent, and data received.



Blocked

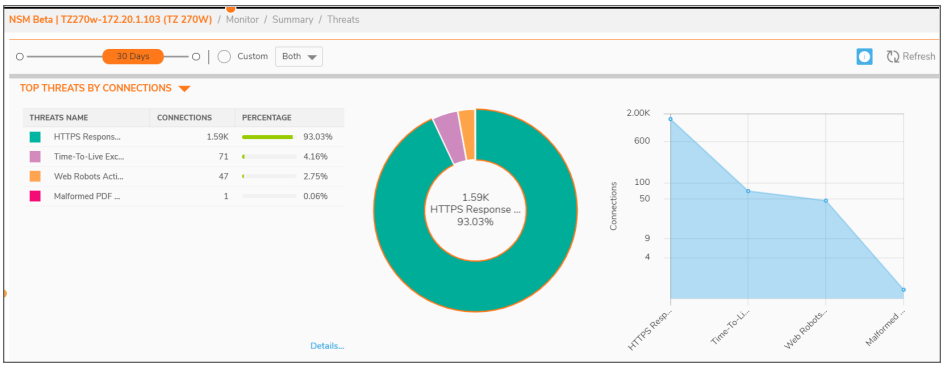
This report tracks the number of blocked connections. The report shows, the number of connections blocked and percentage of them based on Firewall rule, Threat, and Botnet Filter.

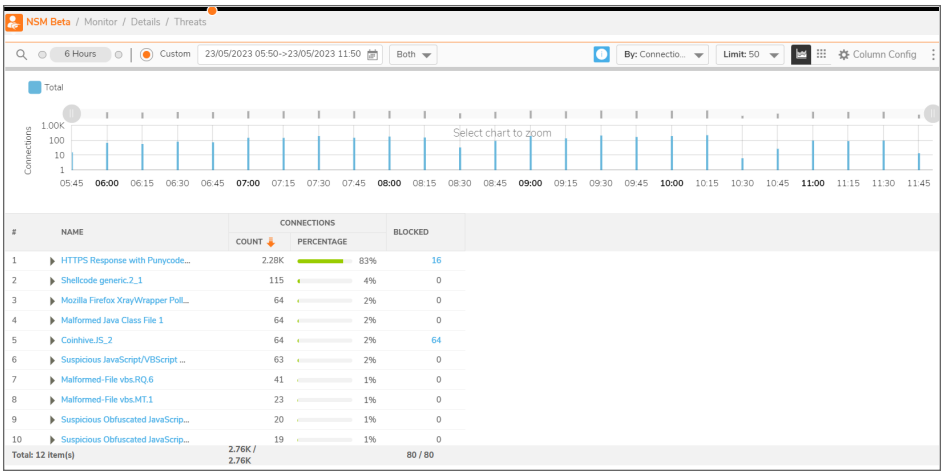




Threats

This report tracks the number of connections with threats. The report shows the number of connections with threats and number of connections blocked. Click on **HOME > System > Threat** to see the threat summary of categories of threats. Two reports are available you can use the drop-down menu to get Threats by Connections and Threats by Blocked.





VPN Reports

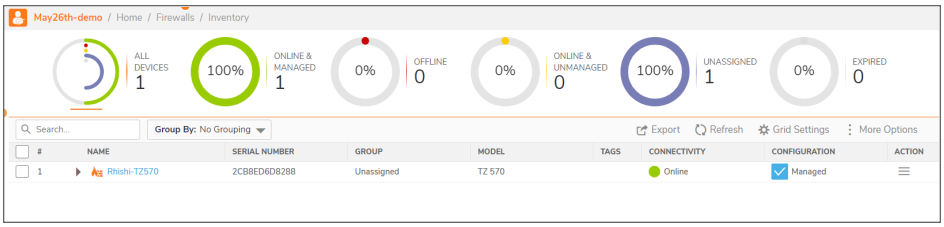
VPN Report tracks the traffic flowing through a pair of firewalls to which you have established a VPN tunnel. For example, if you are working on a local system that is protected by a firewall and you want to access information from a system that is remotely located and is protected by another firewall, then you need to establish a Site-to-Site IPSec VPN Tunnel for this purpose. VPN report tracks this network traffic information that passes through the pair of local and remote firewalls.

The traffic generated by data flowing from local firewall is tracked through **Source VPN** report and the traffic generated by data flowing from remote firewall is tracked through **Destination VPN** report.

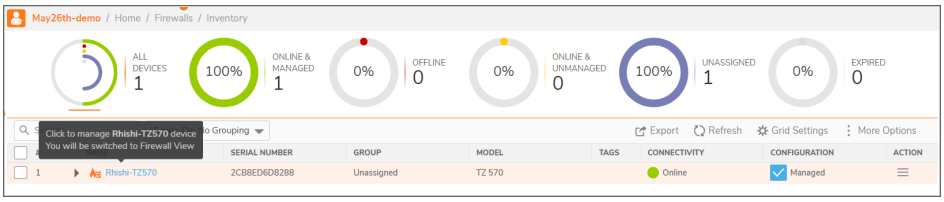
Navigating the VPN Reports

The Source and Destination VPN Reports can be accessed through the **Firewall** view for a specific firewall.

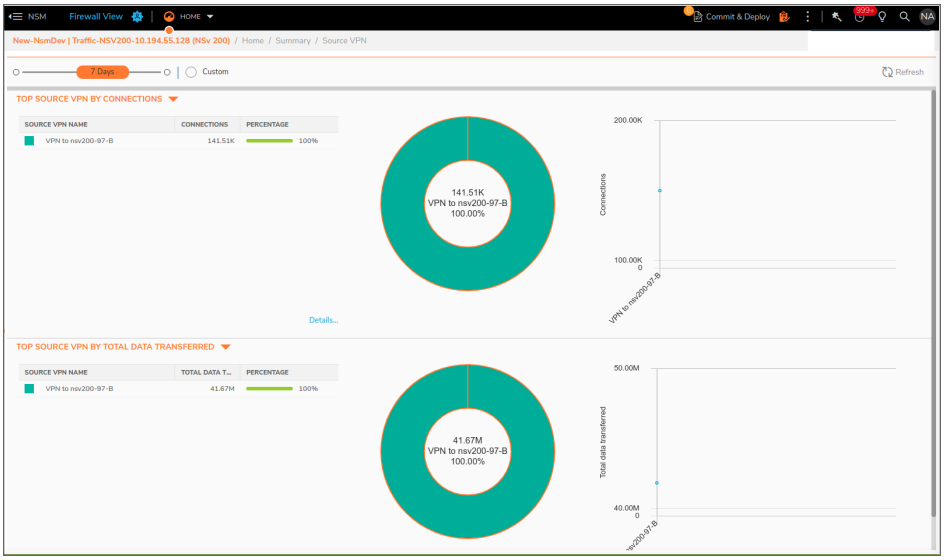
1. Go to **Firewalls > Inventory** to view a list of all the firewall devices.



2. Click on the **Name** of the firewall device for which you want to view the VPN reports. You will be directed to the **Firewall View** for the selected device.



3. Click on **Summary > Source VPN** to view the Source VPN reports page.



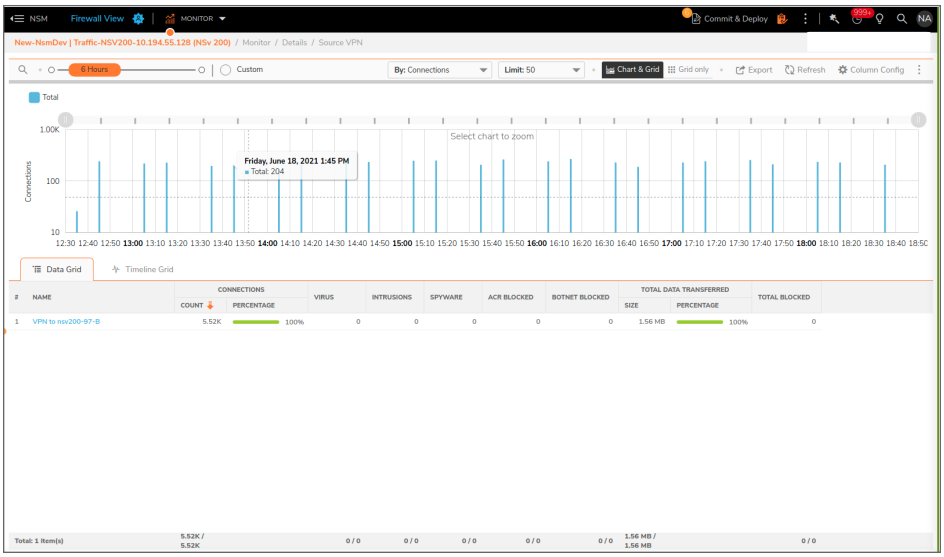
This reports page shows information such as source vpn name, connections and percentage. You can also find the data in the form of a Pie Chart as well as a Graph. The **Time Range** option lets you customize the time duration of the report to show data from the last hour to the last 365 days. You can also use the **Custom** button to customize the dates. The **Refresh** button is used to refresh the page.

This page lets you view 2 sets of report at the same time which can be selected from a list of **By Metrics**:

- Connections
- Total Data Transferred
- Total Connections Blocked
- Intrusions
- Virus
- Spyware
- Connections blocked by Botnet Filter
- Connections blocked by Access Rule
- Connections blocked by GeoIP Filter
- Connections blocked by Threats
- Connections blocked by CFS service

- Connections blocked by App Rule
- Data Sent
- Data Received

4. Click on **Details**, below each report, to go to the details page of the VPN report. You can also view the page by selecting **Monitor** view at the top of the page and navigating to **Details > Source VPN**.



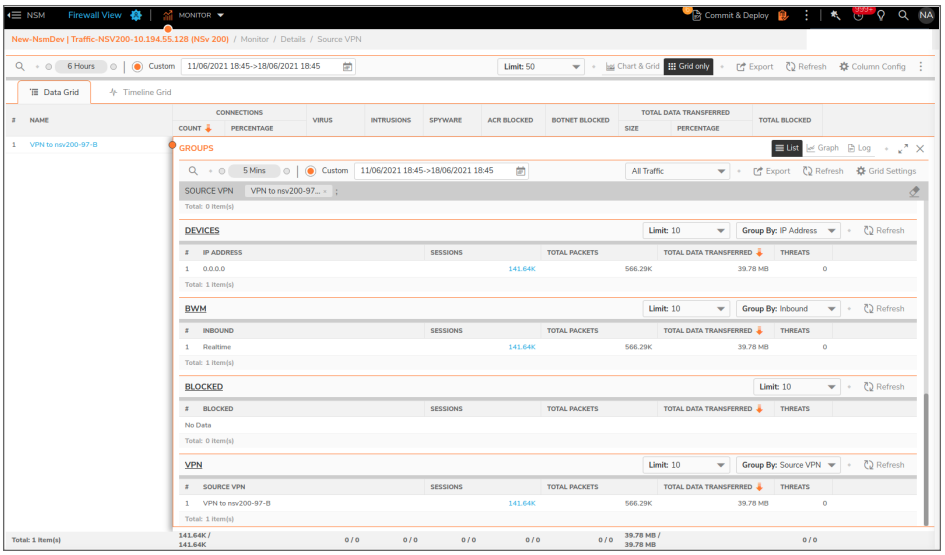
The top of the **Details** page shows a graphical representation of the selected **By Metric** data over a time period. You can change the information on the graph according to the above mentioned By Metric list by using the drop down button, at the top of the page. You can also hover above the graph to see more information.

You have a **Time Range** option that lets you customize the time duration of the report. The **Limit** drop down is used to set the limit of the number of displayed firewall device. You can further filter the graph according to a specific time by using the **Time Slider** which is present above the graph.

You can also click on **Refresh** button to refresh the information on the page and export the table in CSV format using the **Export** button.

The bottom of the page has a table that shows information such as name of the source vpn, connections and total data transferred. The rest of the columns of the table can be selected from the **Column Config** button at the top of the page. The total information of each column can be seen at the extreme bottom of the page.

5. Click on the **Search** icon next to the name of the firewall to see drill down to groups information.



NOTE: You can view and generate a similar report for the destination firewall by selecting the **Destination VPN** page under Summary.

5

Analytics

The Analytics section provides the tools to evaluate data collected by the firewall ecosystem, make policy decisions and take defensive actions using application- and user-based analytics.

ⓘ | **NOTE:** You need to have NSM advance license to view and manage the Analytics.

- About Analytics
- Navigating to the Analytics Page
- Custom Filters

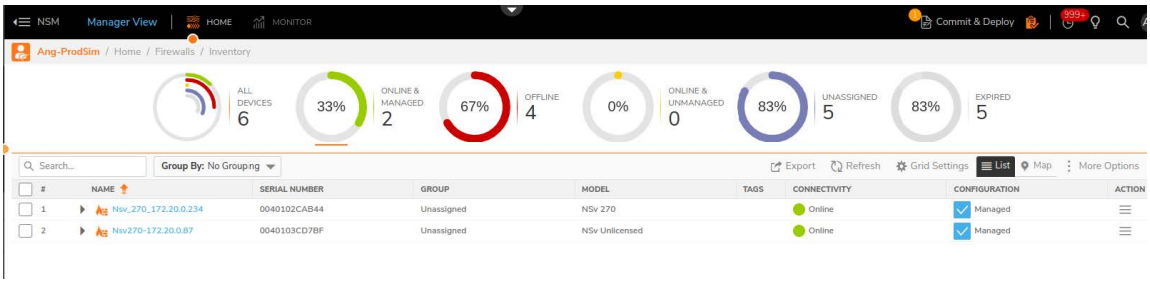
About Analytics

Analytics gives user ability to perform deep investigation on traffic going through firewall. Information collected from firewall is visualized in the form of groups, graphs and table for simple and effortless investigation. Analytics can be performed on all firewall logs or logs related to specific report.

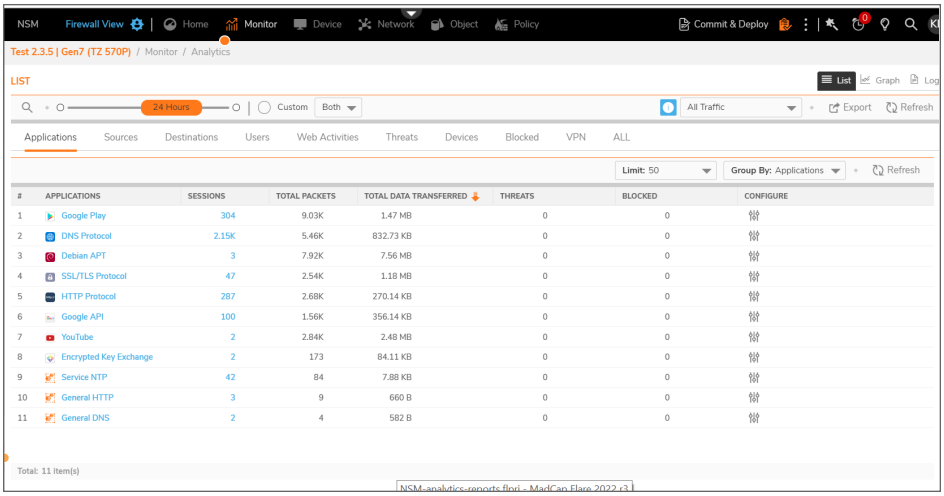
Analytics gives detailed insight of user information such as network events, user activities, threats, operational and performance issues, security efficacy, risks and security gaps, compliance readiness, and auditing. You can perform flexible drill-down and gain insight into your network, user access, connectivity, application use, threat profiles, and other firewall-related data.

Navigating to the Analytics Page

1. Go to **Firewalls > Inventory** to view a list of all the firewall devices.



2. Click on the **Name** of the firewall device for which you want to view the analytics data. You will be directed to the **Firewall View** for the selected device.
3. Click on the **Analytics** tab on the Monitor view to view the **Analytics** page.



List View

The Anaytics page displays the session log data in 3 views i.e. **List, Graph and Log**. When you click on the Analytics tab you will be directed to the list view by default. This view groups all data in different tabs on your selected firewall network such as Applications, Source and Destination IP Addresses, Users, Web Activities, Threats, Devices, BMW, Blocked and VPN. The **ALL** tab allows you to view all combinations of analytics list view. You can click on each application to see additional information regarding the application.

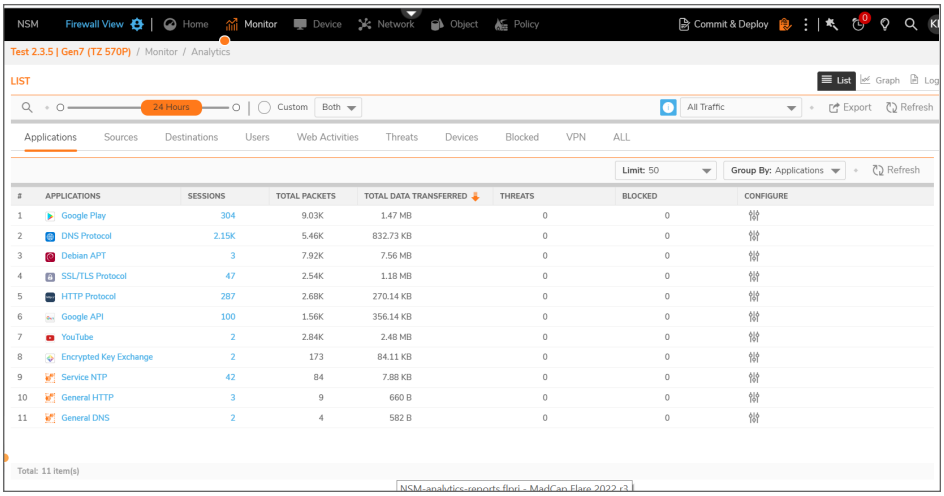
There is a **Blocked** column in each tab that provides drill down information to blocked sessions/connections.

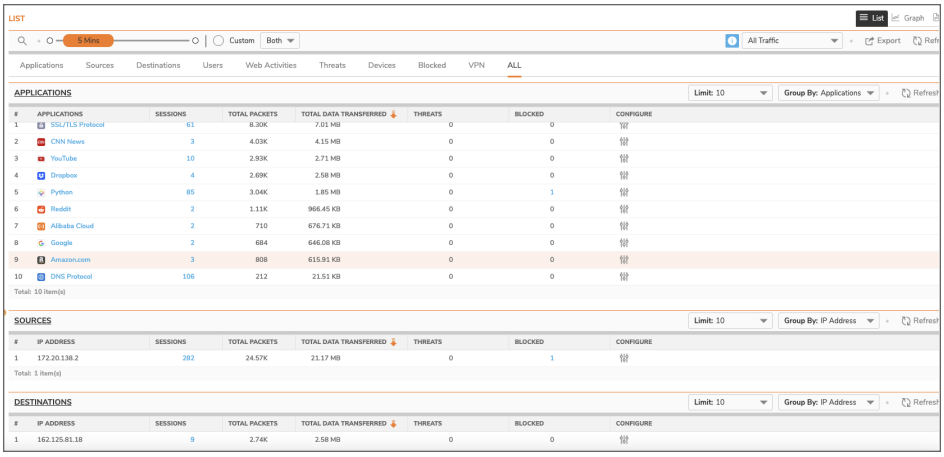
This view can be customized by modifying limit or number of rows displayed in each group, modifying default 'group by' and displayed columns. You can click on sessions to view specific session logs.

You can filter the information according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

You can use the **Search** button to search for a particular application as well as use the **Time Slider** to adjust the time duration. You can also use the **Custom** button to customize the dates. The **Traffic Type** drop down button allows you to select the report type. You can also export the data using the **Export** button and refresh the page using the **Refresh** button.

Apart from the above functions you can filter on any value within group such as in below screen shot you can filter on SSL application by clicking on funnel icon that appears on hovering the mouse in empty space after the application name. Once you filter on specific application name and reload the view, data present in all other groups is filtered for selected values. So, if you filter application by SSL and reload the page, values in sources will display only SSL application sources. This is applicable for all other groups as well i.e. destination, users, etc.





Graph View

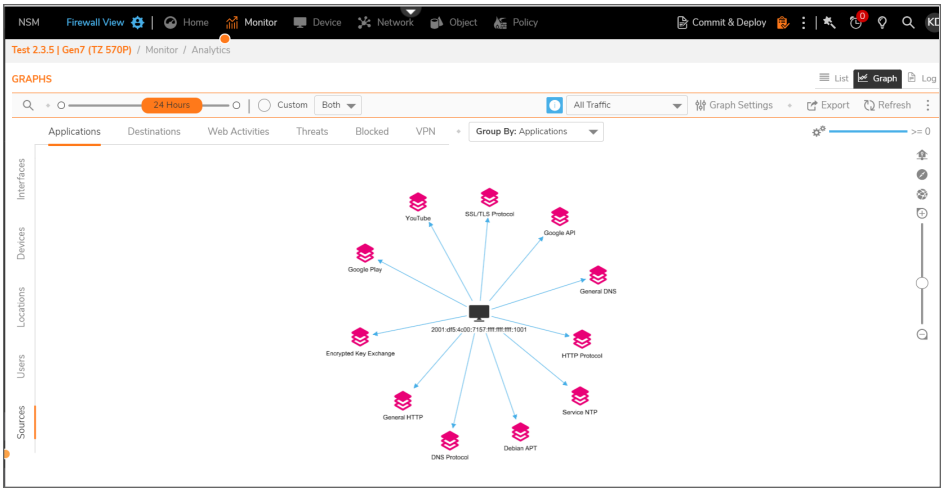
This view allows you to see the relationship between any two metrics available on X and Y, in a graphical format. You can change the individual metric by clicking on the different options on the X and Y axis. For example, if you

want to see which all Source IP are generating traffic for specific Application, then you can choose Sources on Y axis and Application on X axis.

The **Zoom Slider** on the right allows you to zoom in and out of the graph. The **Report Type** drop down button allows you to select the report type. You can also export the data using the **Export** button and refresh the page using the **Refresh** button.

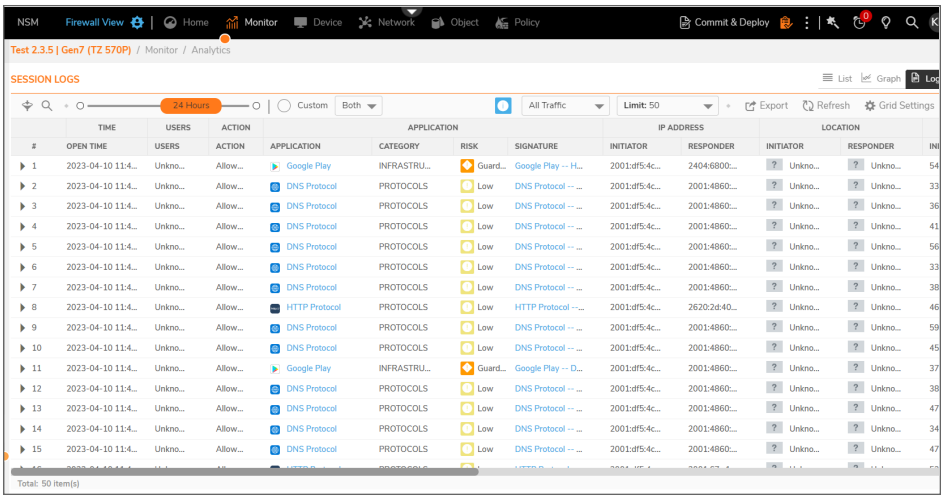
You can filter the information according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

Above the graph, you can change the **Group By** information using the drop down button. You can also change the visual elements of the graph by using the **Graph Setting** Button.



Log View

This view allows you to see the list of individual connections going through your firewall. You can expand each connection to see more details regarding the connection such as Flow Details, IP/Port Information, Statistics, Application/Threats and Additional Details.



You can use the **Search** button to search for a particular information. The **Search** button also allows you to search multiple IP adresses at the same time using the **CIDR** method. For example, you can search 142.250.0.0/16 to see all the subnets under the series 142.250. You can also search 142.250.196.0/24 to see all the subnets under the series 142.250.196.

You can use the **Time Slider** to adjust the time duration and the **Custom** button to customize the dates. The **Traffic Type** drop down button allows you to select the report type. You can also export the data using the **Export** button and refresh the page using the **Refresh** button.

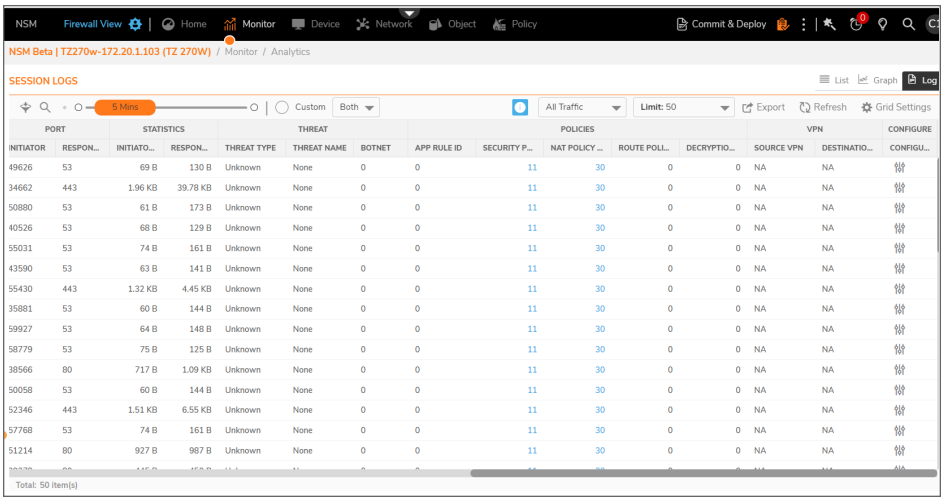
You can filter the information according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

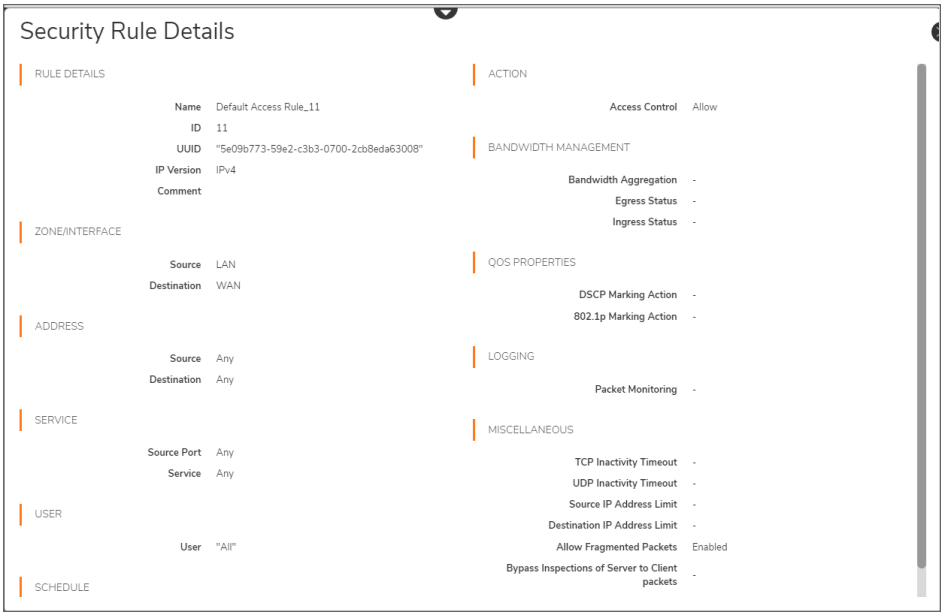
The **Limit** drop down is used to set the limit of the number of connections. You can also edit the columns of the table by using the **Grid Settings** Button.

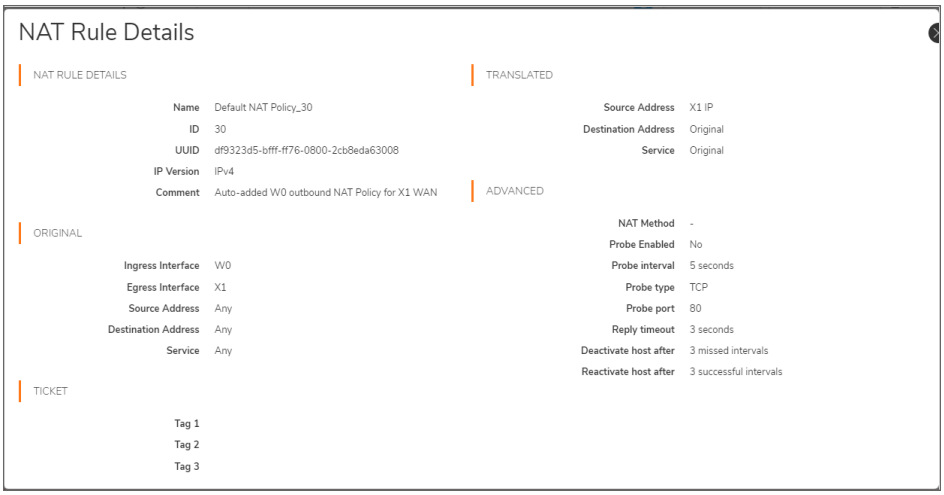
This view allows you to create **Custom Filters** as well.

Policy ID

There is a **Policy ID** column in the log view that allows you to enable debugging based on policies for a selected session. You click on hyper linked policy ID to know more details about rule/policies applied on a selected session.


NSM
Firewall View
Home
Monitor
Device
Network
Object
Policy
Commit & Deploy
NSM Beta | TZ270w-172.20.1.103 (TZ 270W) / Monitor / Analytics
SESSION LOGS
List
Graph
Log
5 Mins
Custom
Both
All Traffic
Limit: 50
Export
Refresh
Grid Settings
PORT
STATISTICS
THREAT
POLICIES
VPN
CONFIGURE
INITIATOR
RESPON...
INITIATO...
RESPON...
THREAT TYPE
THREAT NAME
BOTNET
APP RULE ID
SECURITY P...
NAT POLICY ...
ROUTE POLI...
DECRYPTIO...
SOURCE VPN
DESTINATIO...
CONFIGU...
49626 53 69 B 130 B Unknown None 0 0 11 30 0 0 NA NA
34662 443 1.96 KB 39.78 KB Unknown None 0 0 11 30 0 0 NA NA
50880 53 61 B 173 B Unknown None 0 0 11 30 0 0 NA NA
40526 53 68 B 129 B Unknown None 0 0 11 30 0 0 NA NA
55031 53 74 B 161 B Unknown None 0 0 11 30 0 0 NA NA
43590 53 63 B 141 B Unknown None 0 0 11 30 0 0 NA NA
55430 443 1.32 KB 4.45 KB Unknown None 0 0 11 30 0 0 NA NA
35881 53 60 B 144 B Unknown None 0 0 11 30 0 0 NA NA
59927 53 64 B 148 B Unknown None 0 0 11 30 0 0 NA NA
58779 53 75 B 125 B Unknown None 0 0 11 30 0 0 NA NA
38566 80 717 B 1.09 KB Unknown None 0 0 11 30 0 0 NA NA
50058 53 60 B 144 B Unknown None 0 0 11 30 0 0 NA NA
52346 443 1.51 KB 6.55 KB Unknown None 0 0 11 30 0 0 NA NA
57768 53 74 B 161 B Unknown None 0 0 11 30 0 0 NA NA
51214 80 927 B 987 B Unknown None 0 0 11 30 0 0 NA NA
Total: 50 item(s)


Security Rule Details
RULE DETAILS
Name Default Access Rule_11
ID 11
UUID "5e09b773-59e2-c3b3-0700-2cb8eda63008"
IP Version IPv4
Comment
ZONE/INTERFACE
Source LAN
Destination WAN
ADDRESS
Source Any
Destination Any
SERVICE
Source Port Any
Service Any
USER
User "All"
SCHEDULE
ACTION
Access Control Allow
BANDWIDTH MANAGEMENT
Bandwidth Aggregation -
Egress Status -
Ingress Status -
QOS PROPERTIES
DSCP Marking Action -
802.1p Marking Action -
LOGGING
Packet Monitoring -
MISCELLANEOUS
TCP Inactivity Timeout -
UDP Inactivity Timeout -
Source IP Address Limit -
Destination IP Address Limit -
Allow Fragmented Packets Enabled
Bypass Inspections of Server to Client packets -

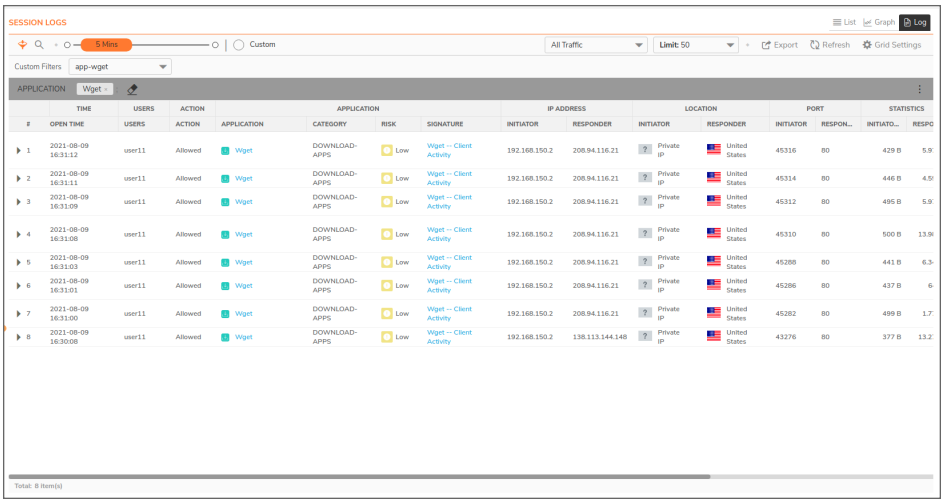


Custom Filters

This feature allows you to create customized filters as per your requirements. This custom filters can be used to manage other reports such as Custom Reports. Custom filters can be created from the **Session Logs** page on the **Monitor View**.

Creating Custom Filters

1. Click on **Analytics** tab on the **Monitor View** to see the Session Log information.

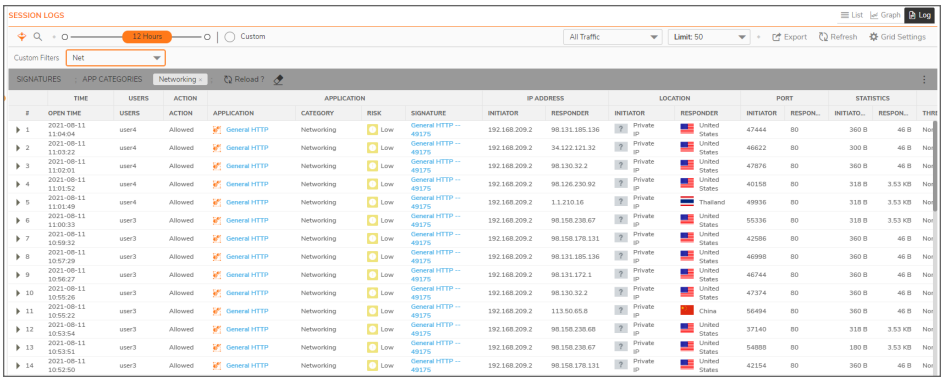


2. Click on the **Filter** symbol next to the columns to filter the information on the table. For example, if you want to view the social networking category information then click on the filter symbol next to **Social-**

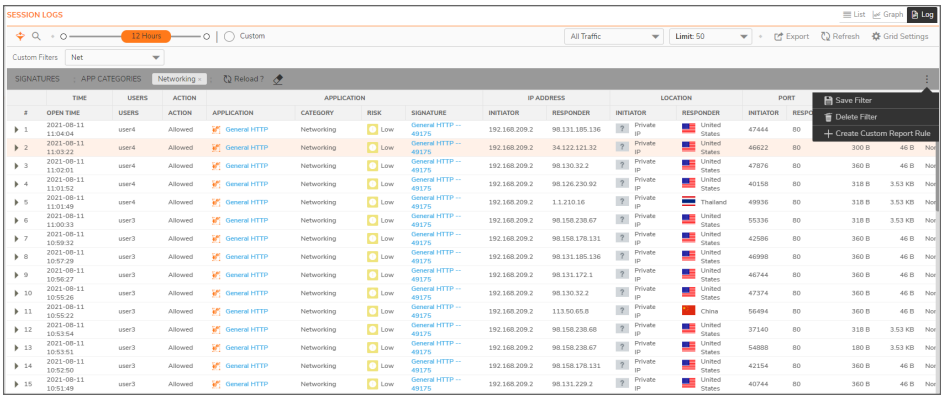
Networking on the **Category** column. Click on **Reload** at the top of the table to filter the table as per the Social-Networking data.

All the existing filter will appear as a drop down when you click on the **Filter** symbol at the top of the table. You can also search for existing filters by clicking on the **Search** symbol.

ⓘ | **NOTE:** You can add multiple filters to the table.



3. To save the filter, click on the three dots at the top-right of the table and click on **Save Filter**. The **Save Custom Filter As** dialog box appears.



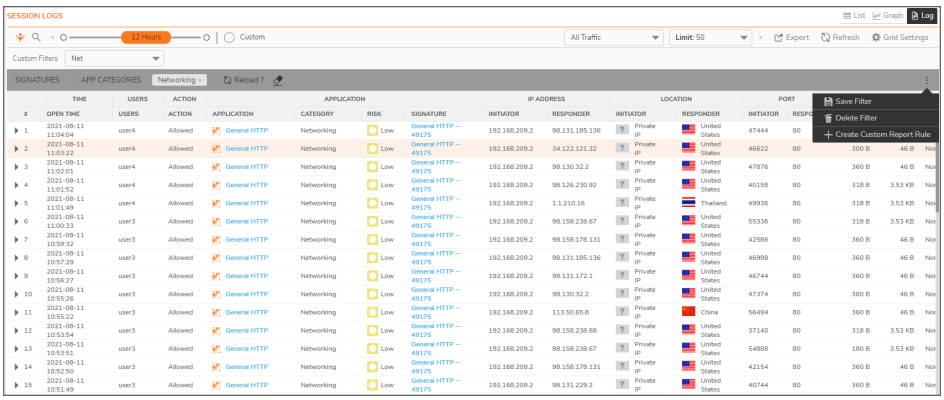
4. Add the **Filter Name** and click on **Save** to save the filter. You can also click on **Save and Create Report Rule** to automatically navigate to the **Custom Reports** page.

Editing and Deleting Custom Filters

You can add or remove individual filters inside a Custom Filter by editing the filter settings.

To add a new filter you need to open the custom filter using the filter option at the top of the table. Then, click on the filter symbol next to the columns to add the filters. Click on the 3 dots at the extreme right and select **Save Filter**. You can remove an existing filter by directly clicking on the **Save Filter** button and removing the filter.

Similarly, you can delete an existing custom filter by clicking on the 3 dots at the extreme right and selecting **Delete Filter**. Once you delete a Custom Filter from the session log page it will also get deleted from the Custom Rules page, which is used to create Custom Report.



6

Log Download

The **Log Download** section provides the tools to download firewall session logs in CSV format. The downloaded session log file can be used for further analysis outside of NSM. You can download session logs by navigating to **Log Download** tab on the **Monitor View**.

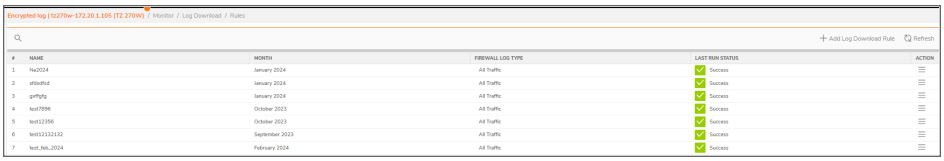
ⓘ | **NOTE:** You need to have NSM advance license to view and manage the Log Download.

ⓘ | **NOTE:** You can download up to 365 days of session logs using Log Download.

Creating Log Download Rule

To download session logs you must first create a log download rule. This allows you to select the information and the time period for which you want to create the log.

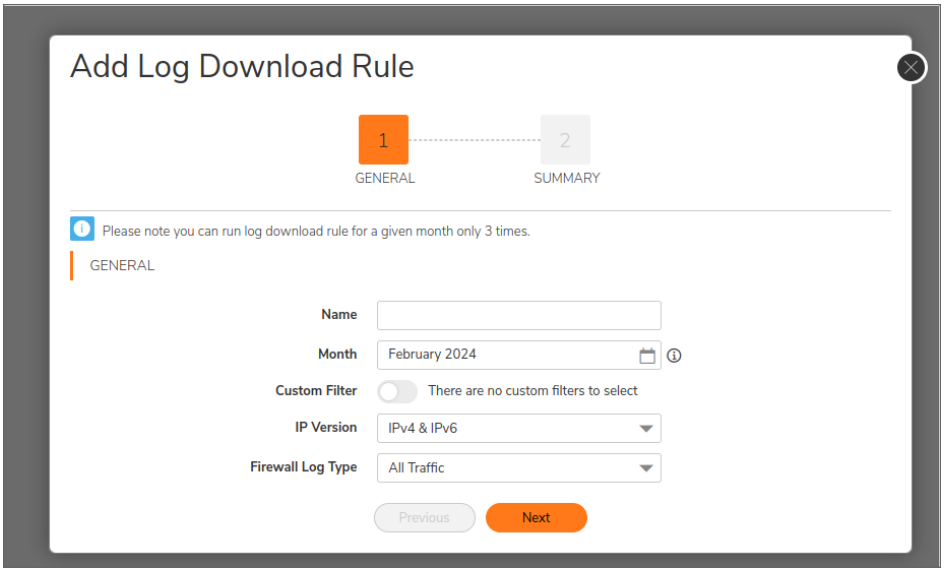
1. Click on the **Name** of the firewall device, under **Firewalls > Inventory**, for which you want to view the session logs. You will be directed to the **Firewall View** for the selected device.
2. Click on **Rules** page on the **Monitor View** to see the list of rules that have been created. You can use the **Search** option to search for an existing rule.

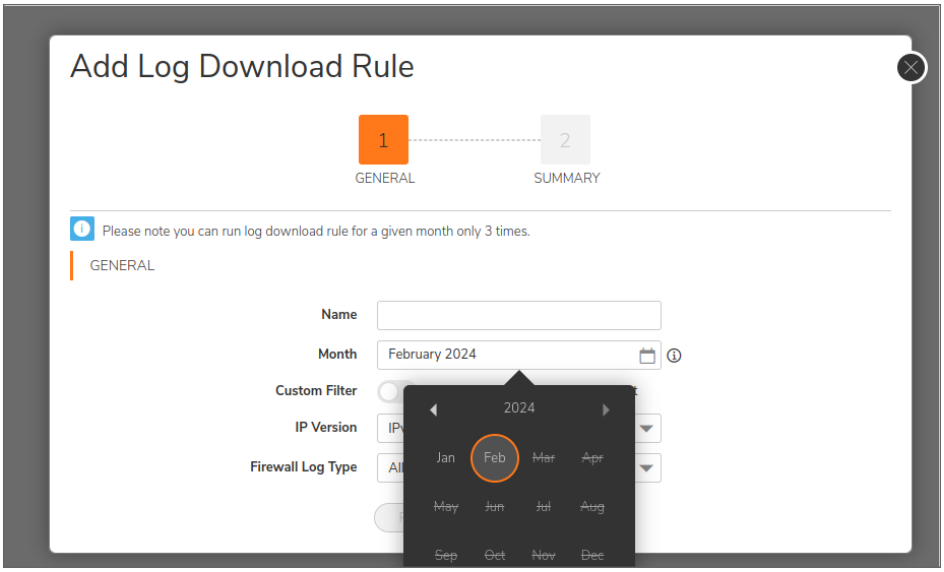


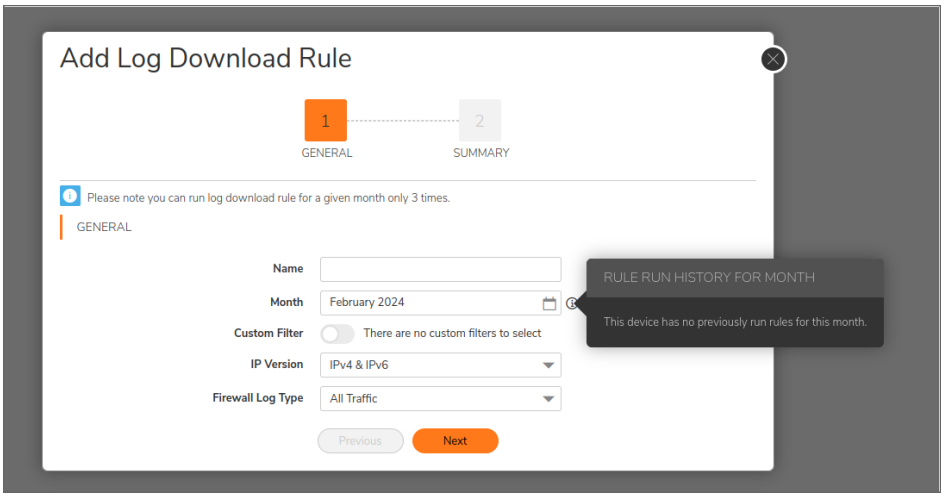
3. Click **Add Log Download Rule** to add a new rule. Fill the following details and click **Next**. You can run log download rule for a given month only **3 times**.
   - **Name:** Enter a name for the log report.
   - **Month:** Select the month for which you want to create the report using the calender option. You can hover on the "i" button to see the date and time stamp as well as the number of times a rule has been run for the selected month.
   - **Custom Filter:** Enable the custom filer toggle to select the custom filter data for your report from the drop down list. You can refer to the Custom Filters section to learn more about how to create and manage custom filters.

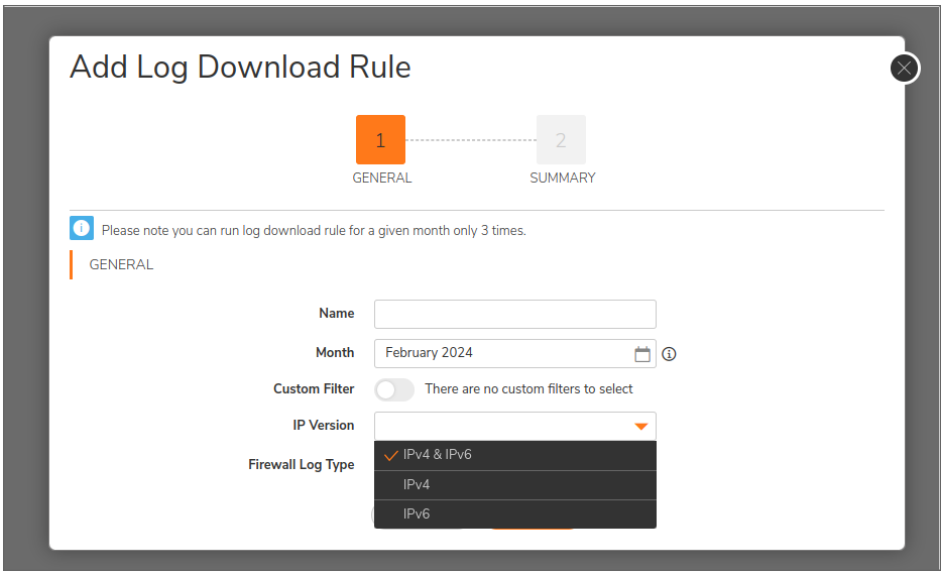
- **IP Version** - Select **IPv4**, **IPv6** or **Both**.
- **Firewall Log Type:** Select the firewall log type as All Traffic, Blocked, Threats or Web Activities.

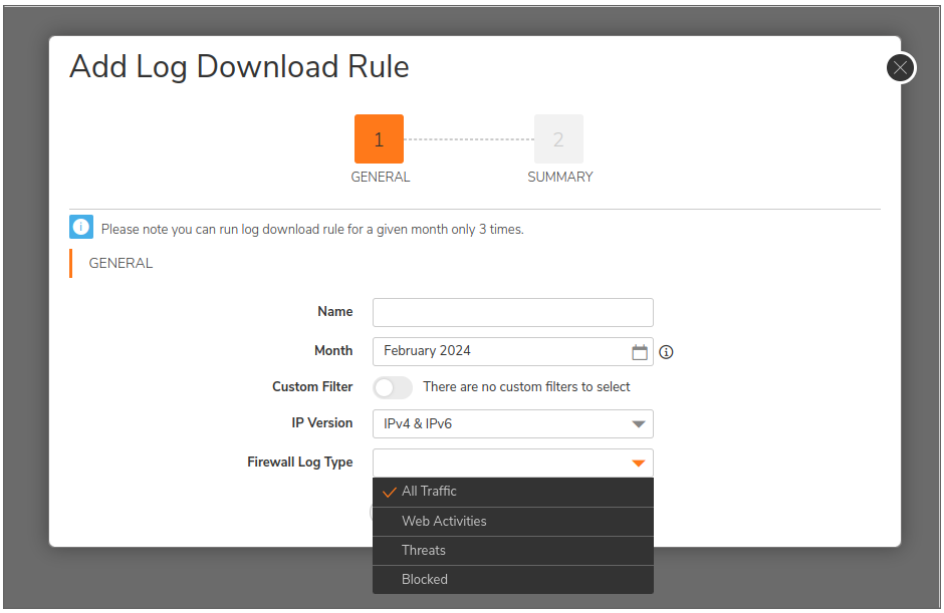
ⓘ | **NOTE:** You need to note the following conditions for downloading Network Traffic Log:



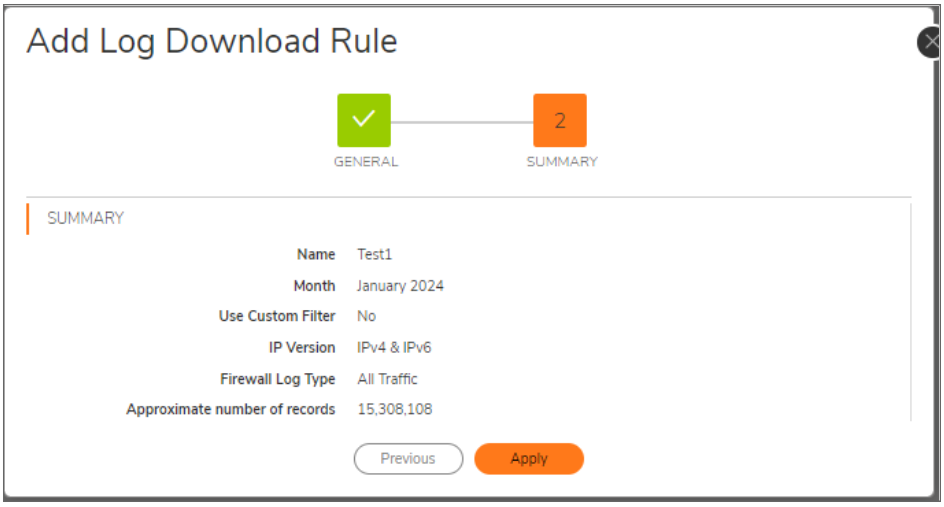



Add Log Download Rule
1
GENERAL
2
SUMMARY
Please note you can run log download rule for a given month only 3 times.
GENERAL
Name
Month
February 2024
Custom Filter
There are no custom filters to select
IP Version
IPv4 & IPv6
Firewall Log Type
All Traffic
Previous
Next
RULE RUN HISTORY FOR MONTH
This device has no previously run rules for this month.


Add Log Download Rule
1
GENERAL
2
SUMMARY
Please note you can run log download rule for a given month only 3 times.
GENERAL
Name
Month
February 2024
Custom Filter
There are no custom filters to select
IP Version
Firewall Log Type
IPv4 & IPv6
IPv4
IPv6

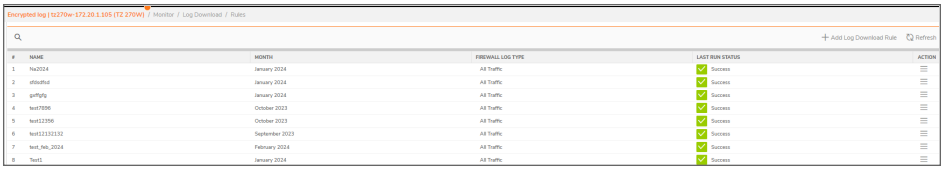


4. On the **Summary** page you can review the data before generating the report. You can also view the approximate number of records to be scanned. Click **Apply** to confirm.



5. After you click Apply, the log download rule is successfully created. Click **Close** to view the rule on the **Rules** page.

6. The new log download rule appears as a new row in the rules page. You can use the Action button to edit or delete the rule.



ⓘ | **NOTE:** You need to note the following conditions for downloading Session Log:

- For current month's rules:

  The Session Log file(s) will contain data for the current month except for the previous two days before today's date. For instance, if you create a rule for downloading the log data for February on the 25th of February, the downloaded data will contain information from the 1st to the 23rd of February.

- For previous month's rules:

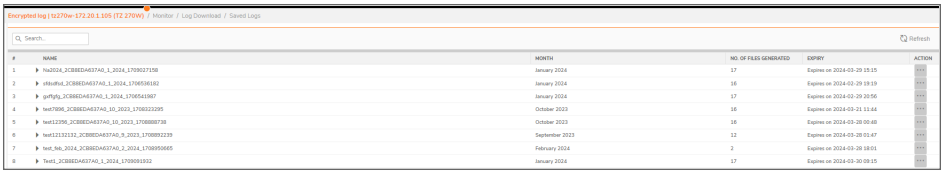
  When you choose any previous month, the downloaded data will contain the entire month's data. For example, if you create a rule for downloading the lLog data for January on the 25th of February, the downloaded data will contain information from the 1st of January to the 31st of January.

Downloading Log File

After you create the Log Download Rule, you can download the log report on the Saved Logs page.

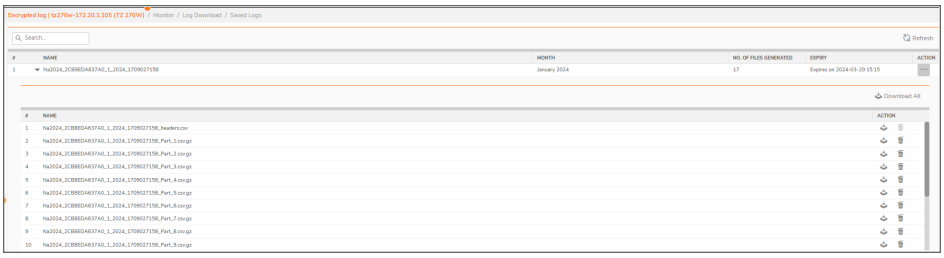
1. Click on the Saved Logs page to view the list of the successfully created log download rule. You can search for a rule using the Search button at the top of the page and delete a rule using the Delete icon at

the right of the page.

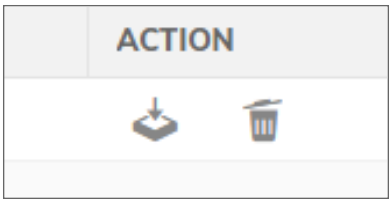


ⓘ **NOTE:** Each log download rule will be available for a month for download. You can see the date and time at which it will get expired under the **Expiry** column.

2. Search for your created rule and expand the row to view the report. If the size of your report is big, then the report will be created in multiple files.



3. Click on Download All to download all the files in the report or click on the Download icon under Actions to download a particular file. You can also delete the report using the delete icon.



4. The report will be successfully downloaded in your system.

ⓘ **NOTE:** There is no restriction on the number of times you can download a generated log

7

Productivity Reports

The **Productivity Reports** section provides the tools to manage productivity reports and view the reports once generated. These reports provide visibility and control of an organization's internet usage. You can also get insightful snapshot of an organization's internet productivity along with details of internet users, websites and web categories.

ⓘ | **NOTE:** You need to have NSM Advance License to view and manage the Productivity Reports.

ⓘ | **NOTE:** The Productivity Report is available at **tenant, group and firewall level**.

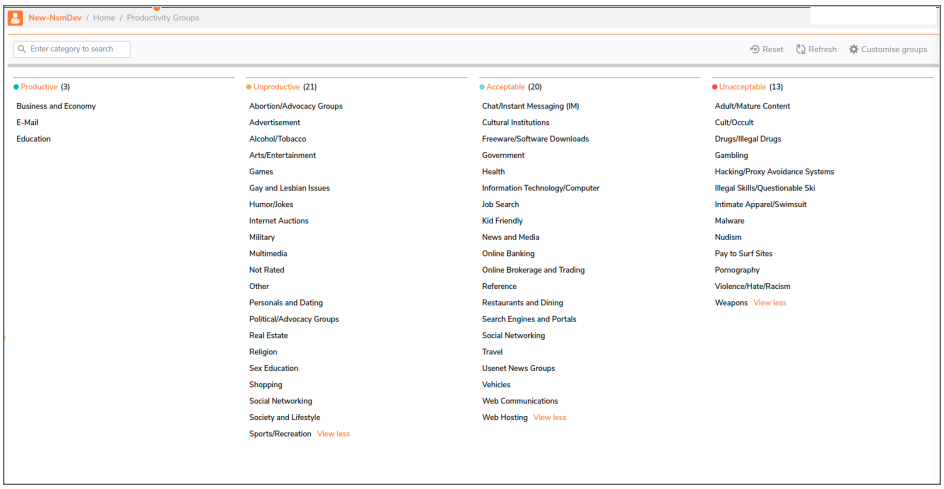
ⓘ | **NOTE:** Tenant and Group level productivity report is available from NSM SaaS **2.3.5** onwards.

Productivity Groups

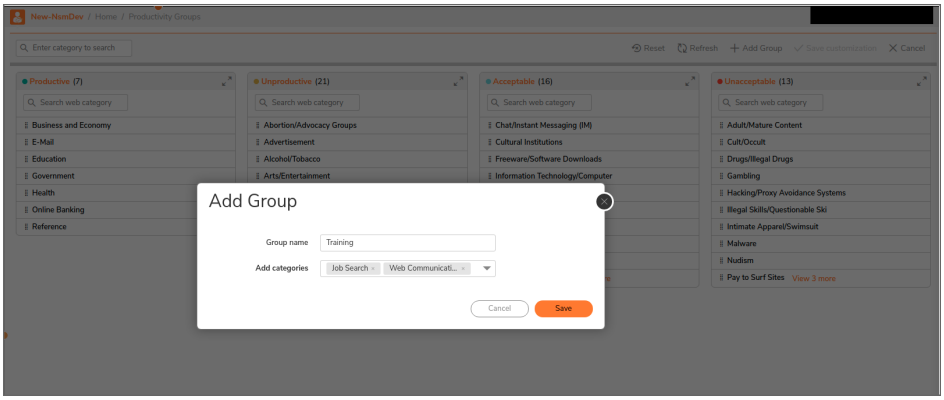
Productivity groups section allows grouping of **Content Filter Service(CFS)** categories. URLs accessed by users is matched first to the CFS and then to the respective productivity groups. There are two types of CFS groups under NSM Productivity Reports i.e. CFS 4.0 and CFS 5.0. Firewalls with SonicOS 7.0.1 firmware or lower support CFS 4.0 and those with SonicOS 7.1.1 firmware or higher support CFS 4.0.

Productivity group configuration is available at tenant level.

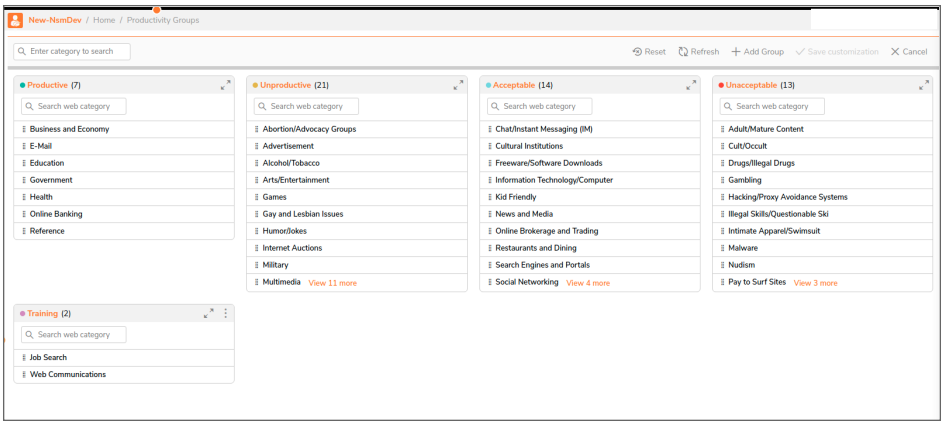
1. Click on **Productivity Groups** tab on the **Manager View** to see the Default group configuration. This list consists of Productive, Unproductive, Acceptable and Unacceptable groups. If you do not see the default groups then you can click on **Reset** button to reset it to default. You can also refresh the page using the **Refresh** button.



2. Click on **Customise groups** button on the top right of this page to make changes to the groups and categories. You can drag and drop the CSF categories to other groups as per your requirement.
3. Click **Add Group** to add a new group. You need to enter a **Group Name** and select the required **Categories**.



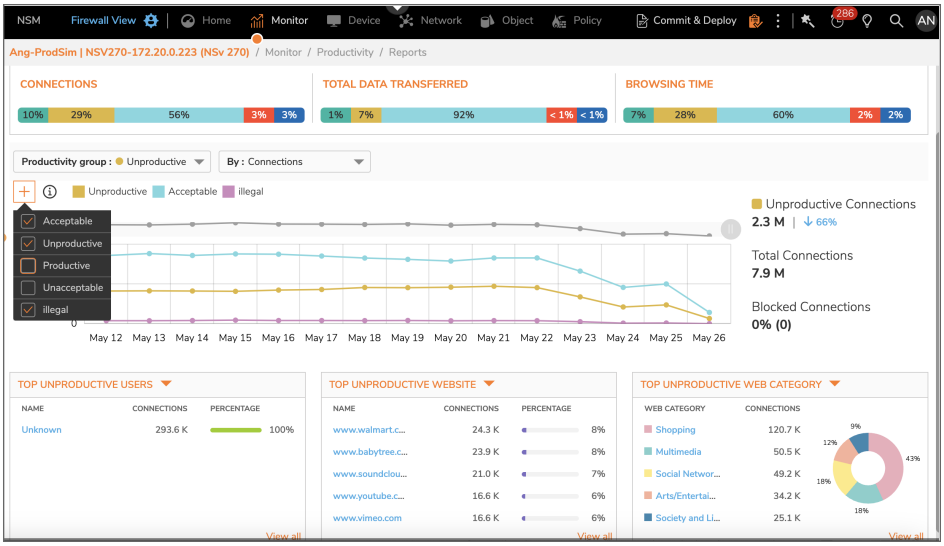
4. Click **Save** to add the new group to the list of existing Productivity groups.



5. You can save the changes by clicking on the **Save Customization** button. You can also select the **Reset** button to reset the groups to default and the **Refresh** button to refresh the page. The **Cancel** button will undo any changes that you may have recently made to the productivity groups.

Navigating to the Productivity Reports Page at Tenant Level

1. Navigate to the **Monitor** page on the **Manager View**.
2. Click on **Productivity > Reports** to view the productivity reports.



ⓘ **NOTE:** You can access Productivity Reports at the Group and Firewall level as well.

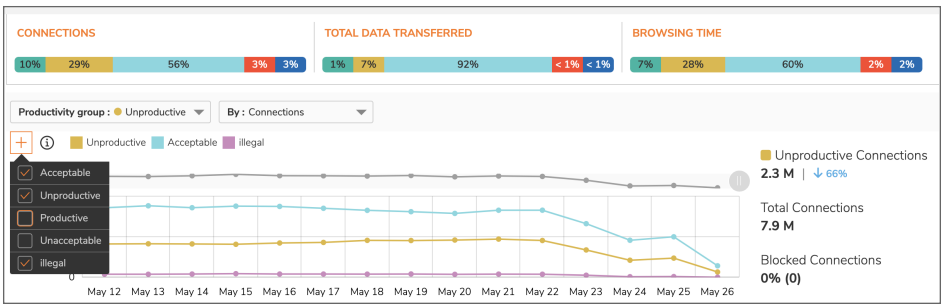
ⓘ **NOTE:** You can do a comparative analysis of various Productivity Group trends by selecting two or more Productivity Groups.

The **Productivity Reports** page shows a graphical representation of total connection / data transferred / browsing time over a time period as well as the top five users, website and web category in a particular productivity group. For example, if the productivity group is selected as unproductive and the By metric is selected as connections, then the graph will display the unproductive connection data and the bottom three sections will show top five unproductive users, websites and web categories.

You can find the color coded chart of the **Summarized Values** across productive categories at the top of the page. The information is divided into three sections, for each By Metric, showing the percentage values of the productive categories as individual colors. You can also find a color legend at the top of the chart which shows the colors assigned for each category. You can hover on the colors to see additional information. The information for all the custom groups will be displayed under a single color.

The top of the reports page displays the following information:

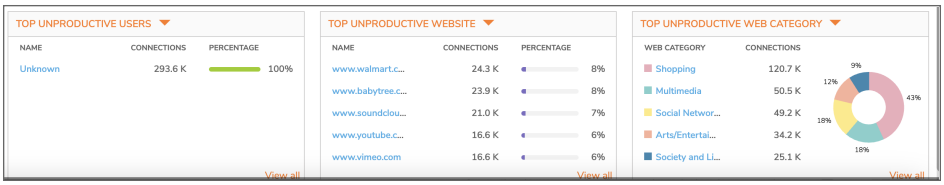
- **Trend Graph** - This graph displays trend of selected productivity category by selected metric. For example if user has selected productive category and metric as data transfer, then this graph displays trend of data transfer in productive category. You can click on the **+ button** to add data for additional productivity groups in the same graph.
- **Time Range** - It is used to customize the time duration of the report to show data from the last hour to the last 90 days. You can also use the **Custom** button to customize the dates.
- **Productivity Group** - This drop down button is used to select the group from a list of productive, unproductive, acceptable, unacceptable or any other custom groups that the user may have created.
- **By Metric** - This drop down button is used to change the information on the graph according to the connections, total data transferred and browsing time.
- **Refresh** - This button is used to refresh the page.
- **Time Slider** - This feature, present above the graph, is used to further filter the graph according to a specific time.
- **Connections Info** - This shows the total connections and the percentage of blocked connections.
- **Trend Comparison** - This shows the percentage increase of a particular metric as compared to the previous time period.



The bottom of the page has three sections that displays the top five list of **Users**, **Website** and **Web Category** along with their respective connections and percentage for a productivity group. You can also change the selection to show top five blocked unproductive users, websites and web category.

You can also view the entire list of items by clicking on **View All** button, where the user will be directed to the respective users, websites and web category page. The items on the list are in the form of hyperlinks which can be clicked to view more information about them.

- **Users** - You can click on each user name to see the list of websites browsed by the user along with additional data about the website such as Web Category, Productivity Category, Connections, Percentage, Browsing Time, Data Transfer and Threats.
- **Website** - You can click on each website to view a list of all the users who have browsed the website along with additional data about the user such as total connections, total data transferred and total browsing time.
- **Web Category** - You can click on each web category to view a list of all the users and websites that belong to this web category.

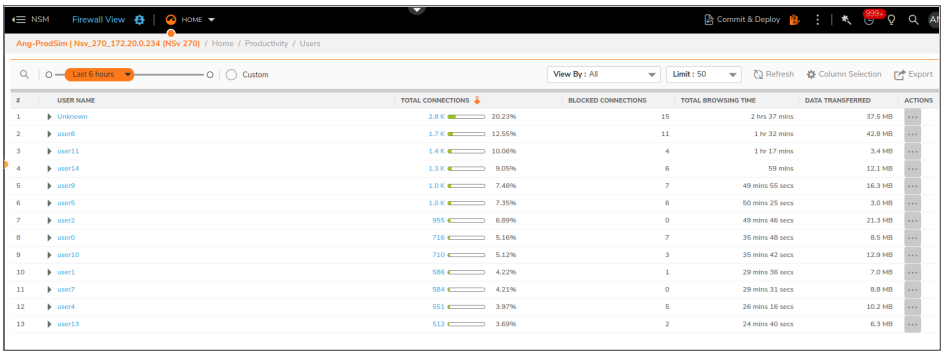


Users

Go to **Productivity > Users** to view a list of all the users who have created the most number of connections. The list can be customized to show data from the last hour to the last 90 days. You can also use the **Custom** button to customize the dates. The **Search** option allows you to search a particular user from the table.

- **User name** - Name of the user.
- **Total connections** - The total connection made by the user. You can click on the data to view drill down information of the session logs.
- **Blocked connections** - The total number of connections that were blocked.
- **Total browsing time** - The total browsing time of the user.
- **Data transferred** - The total data transferred to the website by the user during the browsing time.
- **Actions** - Used to edit the CFS policy and view the drill down to groups information.

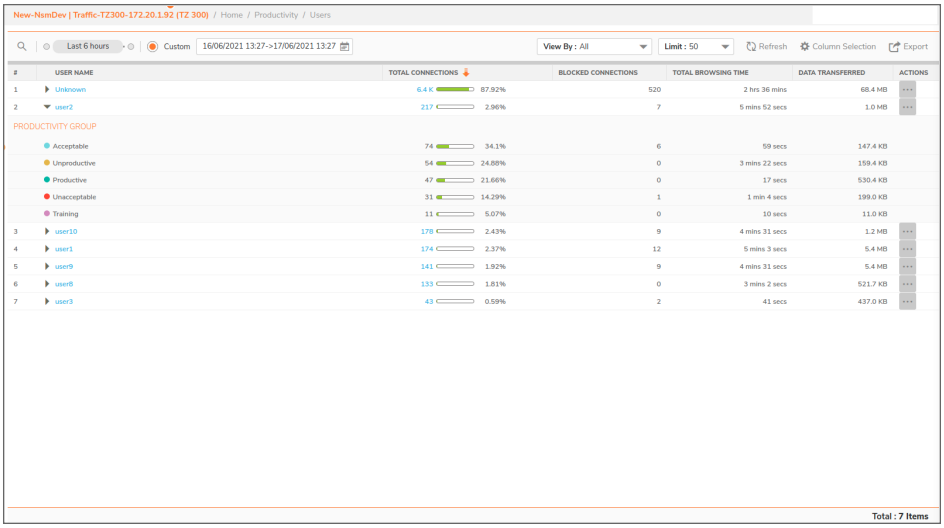
ⓘ **NOTE:** You can change the order of the table according to the column heading by clicking on the **Arrow** symbol besides them.



The **View by** drop down button is used to select the productivity group. The information displayed in the table column changes based on productivity group selected. If you select **All**, then you can see all the productivity group information of all the users, by expanding the name of the user. But If user has selected productive group as unproductive, then values displayed in the total connection, blocked connections, total browsing time and data transferred are for unproductive category only.

All the productivity groups in this drop down feature have been provided different color coded dots for easy identification of the information.

The **Limit** drop down is used to set the limit of the number of displayed users. You can also click on **Refresh** button to refresh the information on the page, edit the columns in the table by the **Column Selection** button and export the table in CSV format using the **Export** button.



Click on the individual **User Name** to see additional browsing information of the user.

At the top of the page, you can see the color coded chart of the **Summarized Values** across productive categories for the selected user. The information is divided into three sections, for each By Metric, showing the percentage values of the productive categories as individual colors. You can also find a color legend at the top of the chart which shows the colors assigned for each category. You can hover on the colors to see additional information. The information for all the custom groups will be displayed under a single color.

You can also change the user and select another user name by using the drop down button at the top of the page.

The top of the table displays user information such as total browsing time, connections and data transferred. You can use the **Limit** drop down to set the limit of the number of displayed websites. You can also use the **Settings** button to refresh the page, edit the columns and export the table.

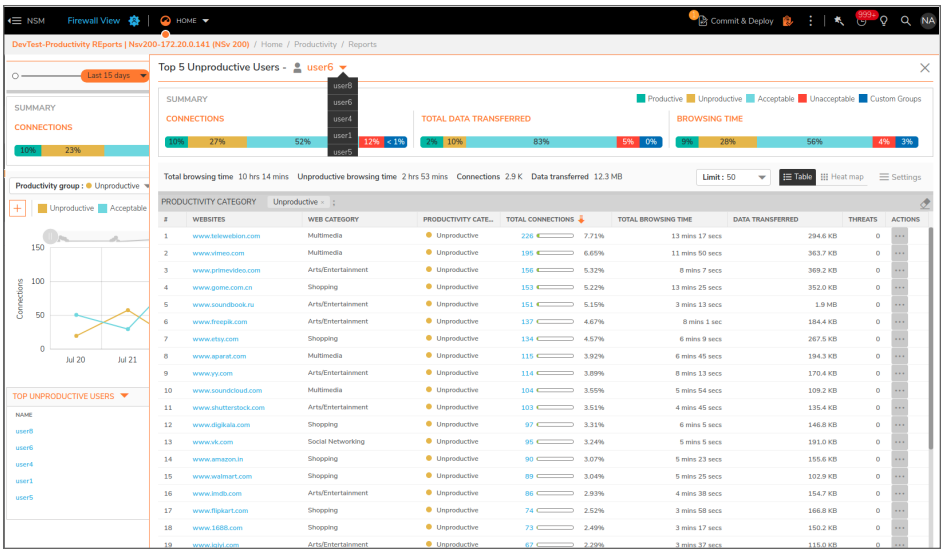
This page also provides you the option to filter the table according to individual web category or productivity category. You can click on the **Filter** symbol besides any of the category and click Reload.

- **Websites** - List of websites browsed by the user.
- **Web category** - Web category to which the website belongs.
- **Productivity category** - Productivity category to which the website belongs.
- **Total connections** - Total connections created for the website. You can click on the data to view drill down information of the session logs.
- **Total browsing time** - Total time that the website was browsed.
- **Data Transferred** - Total data transferred to the website while browsing.
- **Threats** - Total threats detected while browsing the website. You can click on the data to view drill down

information of the threats.

- **Actions** - Used to edit the CFS policy and view the drill down to groups information.

ⓘ **NOTE:** You can click on the **Arrow** symbol besides the total connections, total browsing time or data transferred to change the order of the table.

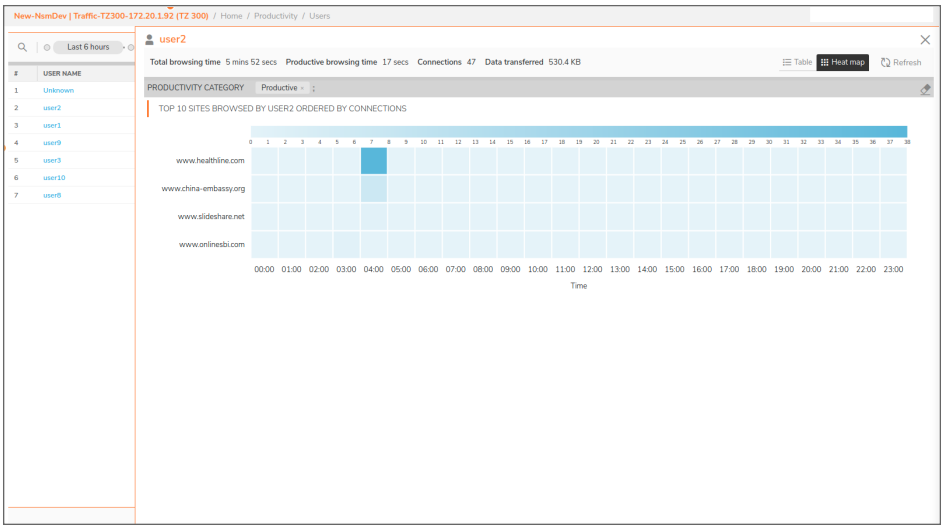


The **Heat Map** is color coded chart that shows the hourly distribution of the top websites that the user has browsed. For example, you can find out browsing pattern of websites during office and non-office hours. The different shades of the heat map represents different amount of data. The darker the shade of the color means the more number of connections have been made for a website at that particular hour. You can hover above the colored box to see more information about the website.

ⓘ **NOTE:** If you have selected the time range of the report for more than 24 hours, 3 days for example, then the heat map will show an aggregate of all the 3 days for that particular hour.

ⓘ **NOTE:** If you have used the filter option on the table view to filter the table according to a web category or productivity category, then the heat map will show only the information related to that filtered category.

ⓘ **NOTE:** If you have changed the order of the table according to a metric, using the Arrow symbol on the table view, then the heat map will show only the information related to that metric



Websites

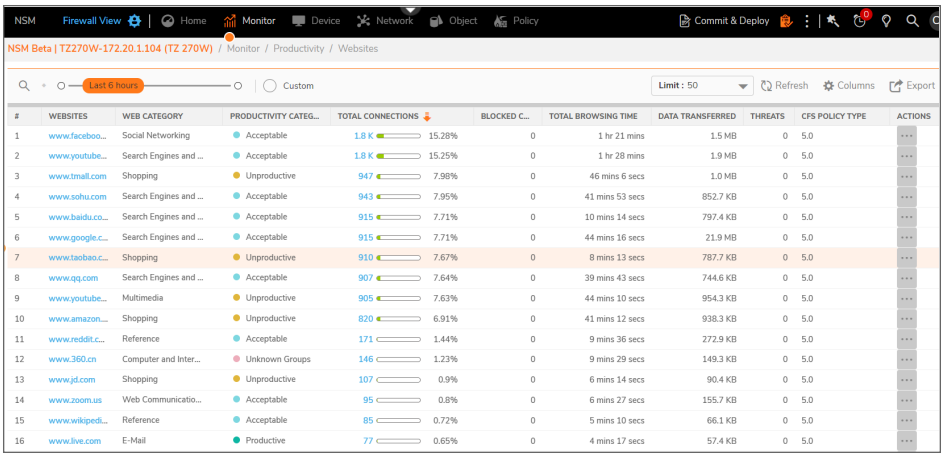
Go to **Productivity > Websites** to view a list of all the websites that have been viewed within the firewall. The list can be customized to show data from the last hour to the last 90 days. You can also use the **Custom** button to customize the dates. The **Search** option allows you to search a particular website from the table.

The **Limit** drop down is used to set the limit of the number of displayed websites. You can also click on **Refresh** button to refresh the information on the page, edit the columns in the table by the **Column Selection** button and export the table in CSV format using the **Export** button.

This page also provides you the option to filter the table according to individual web category or productivity category. You can click on the **Filter** symbol besides any of the category and click Reload.

- **Websites -** List of websites browsed by the user.
- **Web category** - Web category to which the website belongs.
- **Productivity category** - Productivity category to which the website belongs.
- **Total connections** - Total connections created for the website. You can click on the data to view drill down information of the session logs.
- **Total browsing time** - Total time that the website was browsed.
- **Data Transferred** - Total data transferred to the website while browsing.
- **Threats** - Total threats detected while browsing the website. You can click on the data to view drill down information of the threats.
- **CFS Policy Type** - Type of CFS Policy i.e. CFS 4.0 or CFS 5.0.
- **Actions** - Used to edit the CFS policy and view the drill down to groups information.

ⓘ **NOTE:** You can change the order of the table according to the column heading by clicking on the **Arrow** symbol besides them.



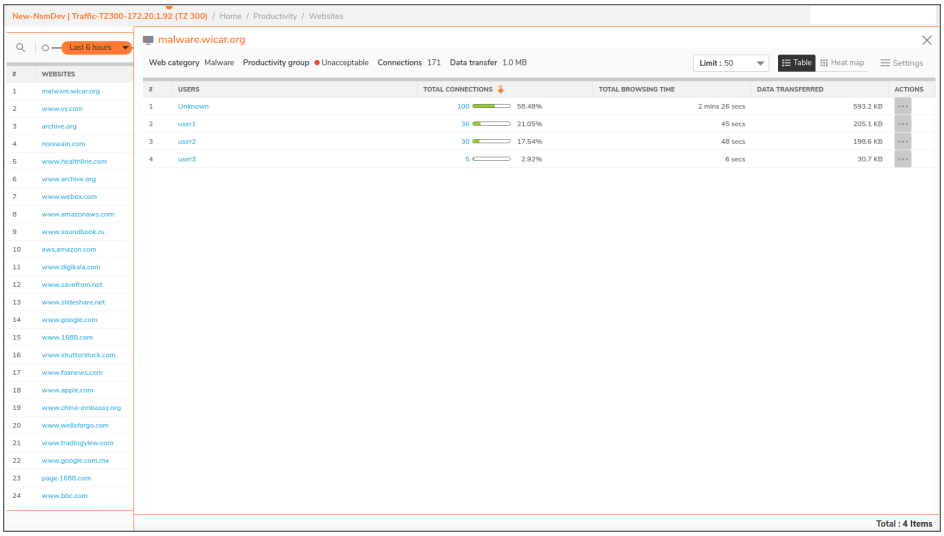
#	WEBSITES	WEB CATEGORY	PRODUCTIVITY CATEG...	TOTAL CONNECTIONS		BLOCKED C...	TOTAL BROWSING TIME	DATA TRANSFERRED	THREATS	CFS POLICY TYPE	ACTIONS
1	www.faceboo...	Social Networking	Acceptable	1.8 K	15.28%	0	1 hr 21 mins	1.5 MB	0	5.0	···
2	www.youtube...	Search Engines and ...	Acceptable	1.8 K	15.25%	0	1 hr 28 mins	1.9 MB	0	5.0	···
3	www.tmall.com	Shopping	Unproductive	947	7.98%	0	46 mins 6 secs	1.0 MB	0	5.0	···
4	www.sohu.com	Search Engines and ...	Acceptable	943	7.95%	0	41 mins 53 secs	852.7 KB	0	5.0	···
5	www.baidu.co...	Search Engines and ...	Acceptable	915	7.71%	0	10 mins 14 secs	797.4 KB	0	5.0	···
6	www.google.c...	Search Engines and ...	Acceptable	915	7.71%	0	44 mins 16 secs	21.9 MB	0	5.0	···
7	www.taobao.c...	Shopping	Unproductive	910	7.67%	0	8 mins 13 secs	787.7 KB	0	5.0	···
8	www.qq.com	Search Engines and ...	Acceptable	907	7.64%	0	39 mins 43 secs	744.6 KB	0	5.0	···
9	www.youtube...	Multimedia	Unproductive	905	7.63%	0	44 mins 10 secs	954.3 KB	0	5.0	···
10	www.amazon....	Shopping	Unproductive	820	6.91%	0	41 mins 12 secs	938.3 KB	0	5.0	···
11	www.reddit.c...	Reference	Acceptable	171	1.44%	0	9 mins 36 secs	272.9 KB	0	5.0	···
12	www.360.cn	Computer and Inter...	Unknown Groups	146	1.23%	0	9 mins 29 secs	149.3 KB	0	5.0	···
13	www.jd.com	Shopping	Unproductive	107	0.9%	0	6 mins 14 secs	90.4 KB	0	5.0	···
14	www.zoom.us	Web Communicatio...	Acceptable	95	0.8%	0	6 mins 27 secs	155.7 KB	0	5.0	···
15	www.wikipedi...	Reference	Acceptable	85	0.72%	0	5 mins 10 secs	66.1 KB	0	5.0	···
16	www.live.com	E-Mail	Productive	77	0.65%	0	4 mins 17 secs	57.4 KB	0	5.0	···

Click on the individual **Websites** to see additional information of the user who has browsed the website.

At the top of the table you can find website information such as web category, productivity group, connections and data transfer. You can use the **Limit** drop down button to set the limit of the number of users. You can also use the **Settings** button to refresh the page, edit the columns and export the table.

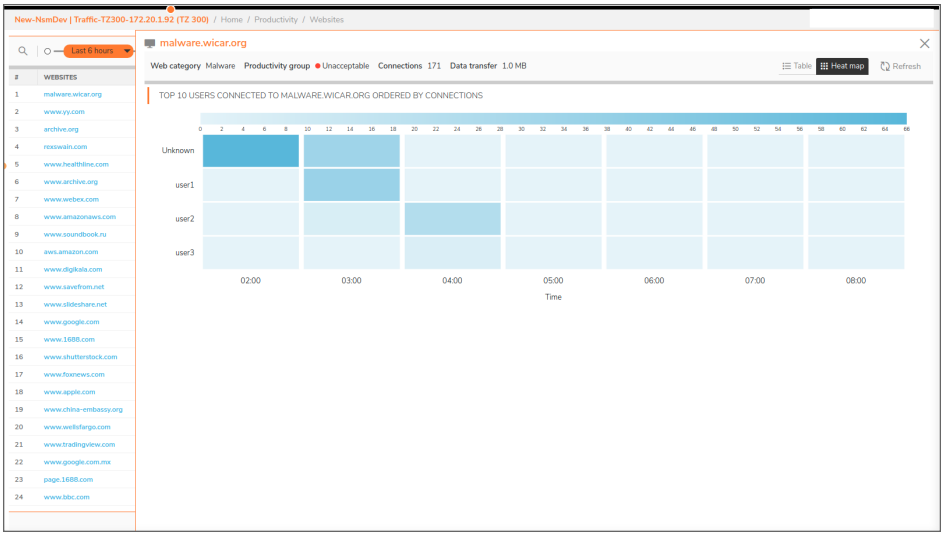
- **User** - Name of the user who has browsed the particular website.
- **Total connections** - The total connection made by the user. You can click on the data to view drill down information of the session logs.
- **Total browsing time** - The total browsing time of the user.
- **Data transferred** - The total data transferred by the user during the browsing time.
- **Actions** - Used to edit the CFS policy and view the drill down to groups information.

ⓘ **NOTE:** You can change the order of the table according to the column heading by clicking on the **Arrow** symbol besides them.



#	USERS	TOTAL CONNECTIONS		TOTAL BROWSING TIME	DATA TRANSFERRED	ACTIONS
1	Unknown	100	58.48%	2 mins 26 secs	593.2 KB	···
2	user1	36	21.05%	45 secs	205.1 KB	···
3	user2	30	17.54%	48 secs	198.6 KB	···
4	user3	5	2.92%	6 secs	30.7 KB	···

The **Heat Map** is color coded chart that shows the hourly distribution of the top users that have browsed the website. To learn more about Heat map, you can check the heat map section under the **User** heading.



Web Categories

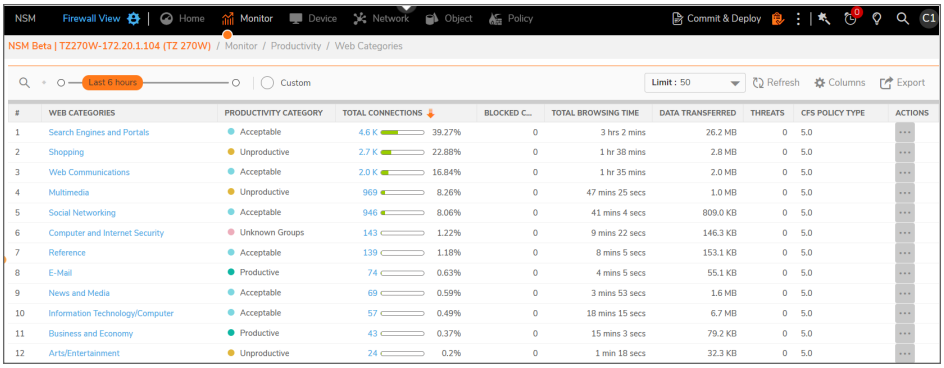
Go to **Productivity > Web Categories** to view a list of all the web categories that have been accessed within the firewall. The list can be customized to show data from the last hour to the last 90 days. You can also use the **Custom** button to customize the dates. The **Search** option allows you to search a particular web category from the table.

The **Limit** drop down is used to set the limit of the number of displayed web categories. You can also click on **Refresh** button to refresh the information on the page, edit the columns in the table by the **Column Selection** button and export the table in CSV format using the **Export** button.

This page also provides you the option to filter the table according to individual productivity category by clicking on the **Filter** symbol next to it.

- **Web category** - Web category to which the website belongs.
- **Productivity category** - Productivity category to which the website in the web category belongs.
- **Total connections** - Total connections created for the web category. You can click on the data to view drill down information of the session logs.
- **Total browsing time** - Total time that the websites in the web category were browsed.
- **Data Transferred** - Total data transferred to the website while browsing..
- **Threats** - Total threats detected while browsing the websites in the category. You can click on the data to view drill down information of the threats.
- **CFS Policy Type** - Type of CFS Policy i.e. CFS 4.0 or CFS 5.0.
- **Actions** - Used to edit the CFS policy and view the drill down to groups information.

NOTE: You can change the order of the table according to the column heading by clicking on the **Arrow** symbol besides them.



#	WEB CATEGORIES	PRODUCTIVITY CATEGORY	TOTAL CONNECTIONS		BLOCKED C...	TOTAL BROWSING TIME	DATA TRANSFERRED	THREATS	CFS POLICY TYPE	ACTIONS
1	Search Engines and Portals	Acceptable	4.6 K	39.27%	0	3 hrs 2 mins	26.2 MB	0	5.0	···
2	Shopping	Unproductive	2.7 K	22.88%	0	1 hr 38 mins	2.8 MB	0	5.0	···
3	Web Communications	Acceptable	2.0 K	16.84%	0	1 hr 35 mins	2.0 MB	0	5.0	···
4	Multimedia	Unproductive	969	8.26%	0	47 mins 25 secs	1.0 MB	0	5.0	···
5	Social Networking	Acceptable	946	8.06%	0	41 mins 4 secs	809.0 KB	0	5.0	···
6	Computer and Internet Security	Unknown Groups	143	1.22%	0	9 mins 22 secs	146.3 KB	0	5.0	···
7	Reference	Acceptable	139	1.18%	0	8 mins 5 secs	153.1 KB	0	5.0	···
8	E-Mail	Productive	74	0.63%	0	4 mins 5 secs	55.1 KB	0	5.0	···
9	News and Media	Acceptable	69	0.59%	0	3 mins 53 secs	1.6 MB	0	5.0	···
10	Information Technology/Computer	Acceptable	57	0.49%	0	18 mins 15 secs	6.7 MB	0	5.0	···
11	Business and Economy	Productive	43	0.37%	0	15 mins 3 secs	79.2 KB	0	5.0	···
12	Arts/Entertainment	Unproductive	24	0.2%	0	1 min 18 secs	32.3 KB	0	5.0	···

Click on the individual **Web Categories** to see additional information of the users and the websites belonging to this web category.

At the top of the table you can find website information such as productivity group, connections and data transfer. You can use the **Limit** drop down button to set the limit of the number of users and websites. You can also use the **Settings** button to refresh the page, edit the columns and export the table.

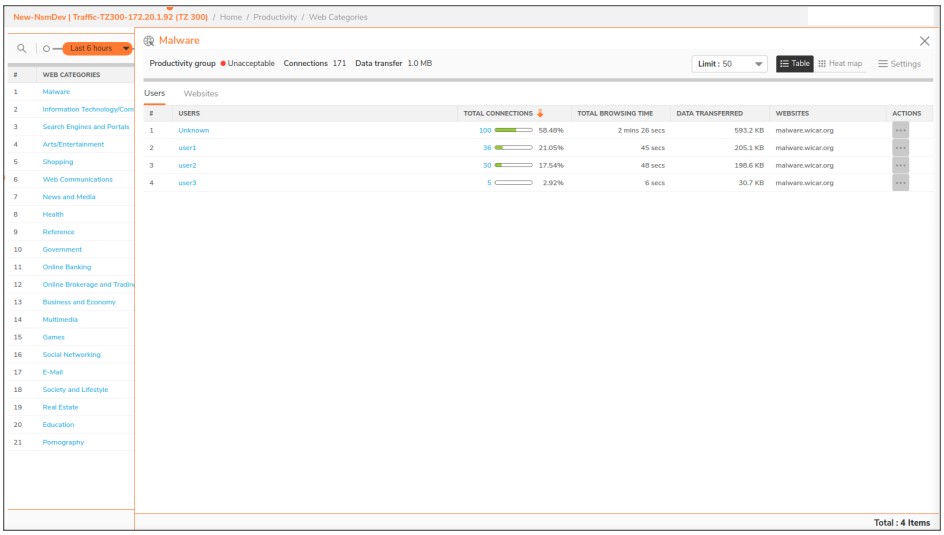
The User table shows the following information:

- **User** - Name of the user.
- **Total connections** - The total connection made by the user. You can click on the data to view drill down information of the session logs.
- **Total browsing time** - The total browsing time of the user.
- **Data transferred** - The total data transferred by the user during the browsing time.
- **Websites** - List of websites browsed by the user.
- **Actions** - Used to edit the CFS policy and view the drill down to groups information.

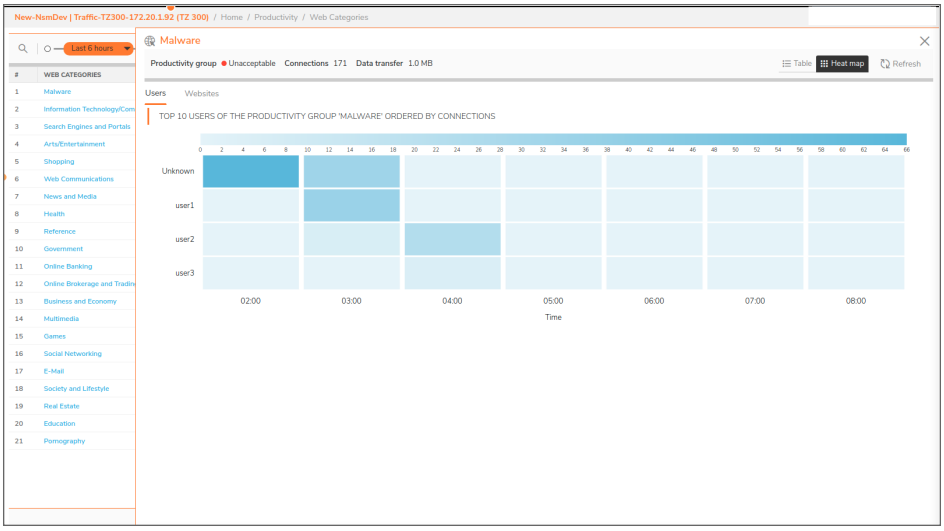
The Websites table shows the following information:

- **Websites** - List of websites browsed in the web category.
- **Total connections** - Total connections created for the website. You can click on the data to view drill down information of the session logs.
- **Total browsing time** - Total time that the website was browsed.
- **Data Transferred** - Total data transferred to the website while browsing.
- **Threats** - Total threats detected while browsing the website. You can click on the data to view drill down information of the threats.
- **Actions** - Used to edit the CFS policy and view the drill down to groups information.

NOTE: You can change the order of the table according to the column heading by clicking on the **Arrow** symbol besides them.



The **Heat Map** is color coded chart that shows the hourly distribution of the top users and websites that have accessed this web category. To learn more about Heat map, you can check the heat map section under the **User** heading.



8

Reports

This chapter provides the information for creating various reports on NSM SaaS. An user can generate reports whose rules can be scheduled or can be created on demand.

There are certain reports that are available at the Device, Tenant and Group level. The below table lists the type of reports that are accessible for the Reports section.

Type of Report	Device Level	Tenant and Group Level
RealTime Monitor and RealTime Report	Available	Not Available
Summary Report and Detailed Report	Available	Available
Analytics	Available	Available
Schedule Report (Default)	Available	Available
Schedule Report (Custom)	Available	Available
Schedule Report (Productivity)	Available	Available
Scheduled reports (CTA)	Available	Not Available
Scheduled reports (Firewall Up-Time Summary)	Available	Available
Download Logs	Available	Not Available

- Capture Threat Assessment (CTA) Report Rules
- Default Report Rules
- Firewall Up-Time Summary Report Rules
- Custom Reports

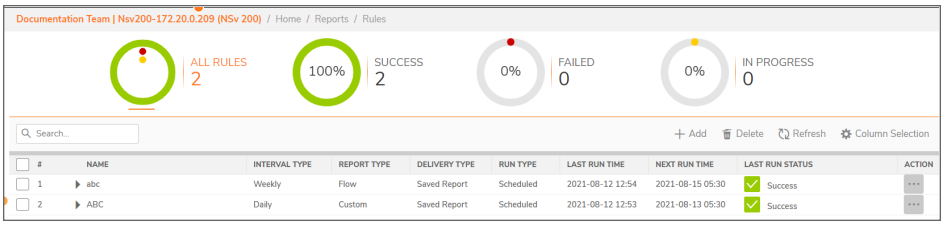
Capture Threat Assessment (CTA) Report Rules

The **CTA Reports Rules** section provides the tools to manage capture threat assessment report rules and view the reports once generated.

ⓘ | **NOTE:** You need to have NSM Advance License to view and manage the CTA Reports.

Navigating the CTA Report Rules Page

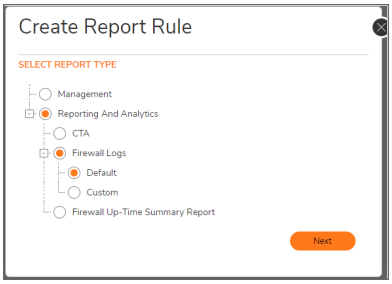
Go to **Reports > Rules** to view a list of all the reports that have been defined. The details of each report are shown in the table.



Setting Up the CTA Report Rule

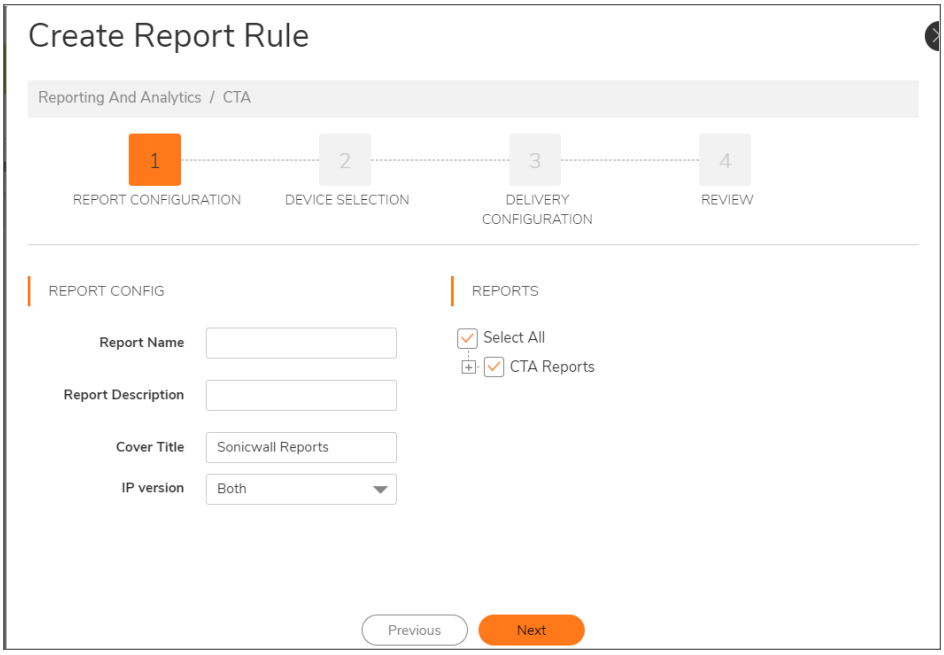
To set up a CTA report rule:

1. Click **Add** above the **Reports** table. Select the **CTA** option and click **Next** to go to the **Report Configuration** page.



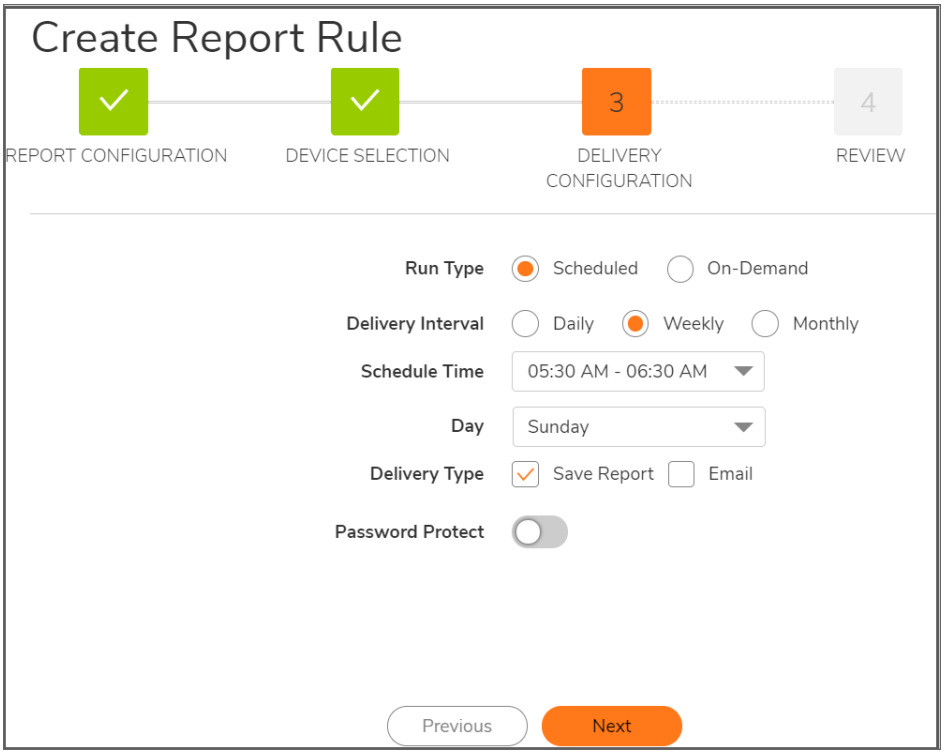
2. Fill the following details in the **Report Configuration** page and click **Next**.
   - **Firewall Name** - It will be the same firewall which you have selected and cannot be edited.
   - **Report Name** - Enter a name for the report.
   - **Report Description** - Enter a description for the report.
   - **IP Version** - Select **IPv4**, **IPv6** or **Both**.

- **Reports** - Select **CTA Reports**.

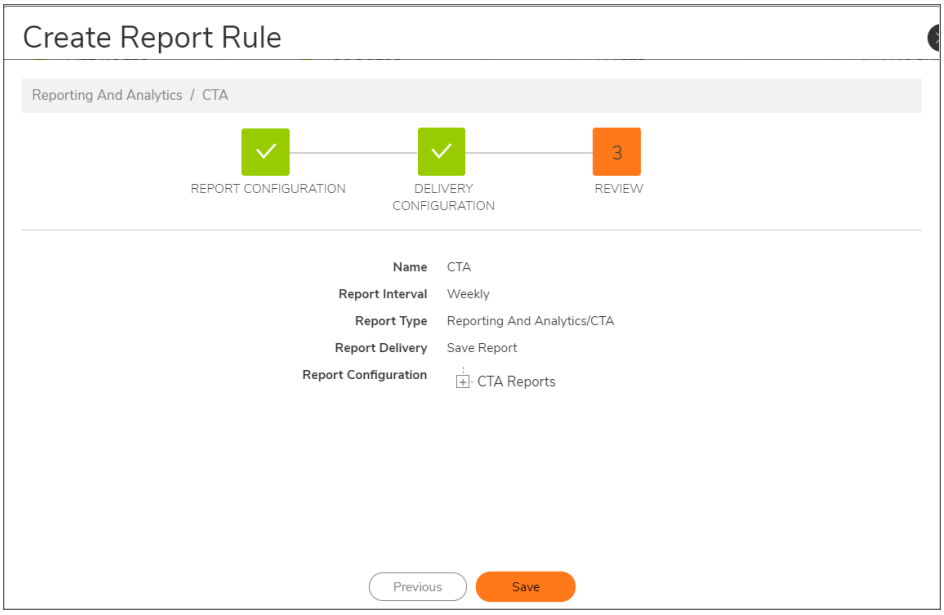


3. On the Delivery Configuration page fill the following information and click **Next**.
   - **On-demand Run Type** - It is used to change the time period of the report using the slider. The maximum report time permissible is 30 days.
   - **Scheduled Run Type** - It is used to choose when the report will be generated for a day, or for selected day of week or selected day of a month.
   - **Delivery Type** - You can select from **Save Report** and **Email** option. Save Report allows you to save the reports in NSM. You can view these saved report in NSM under **Reports > Saved Reports**. Email option allows you to email the report. To email the report you need to select the **Email Destination** as Administrator or Adhoc user. You need to provide the user mail id in the **Email Id** column if you select Adhoc User. You also need to add the **Email Subject** and **Body** as well as select **Zip Report** to send the report in a Zip format.

- **Password Protect** - You can provide a password to the report pdf.



4. On the **Review** page, you can review the data before generating the report. Click **Save** to confirm.



After you click on save, a new CTA rule is created on the **Report Rules** page with your report name.

Default Report Rules

The **Default Report Rules** section provides the tools to manage default report rules and view the reports once generated.

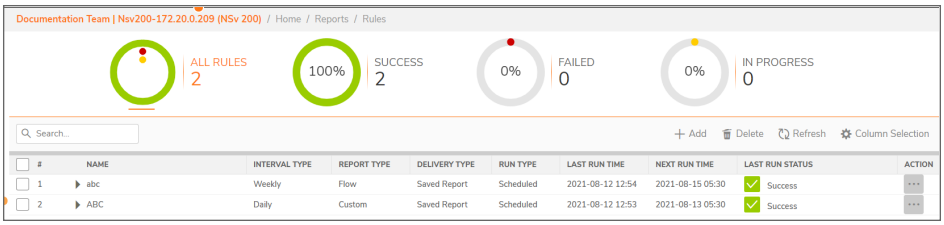
ⓘ | **NOTE:** The **Default Report Rules** feature is the same for both NSM on-prem and SaaS versions.

Managing Default Reports

Several icons at the top right corner of the **Report > Rules** table help you manage your reports. Some restrictions and limits are enforced, and a few additional steps are involved while creating a group-level Default Report. The following examples describe the Manager View. You can view similar reports at firewall and tenant level. Refer to the image and table below to learn more about them.

Navigating the Default Report Rules Page

Go to **Reports > Rules** to view a list of all the reports that have been defined. The details of each report are shown in the table.

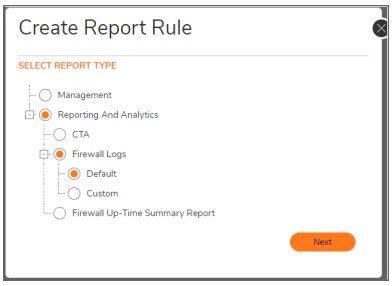


Setting Up the Report Rule

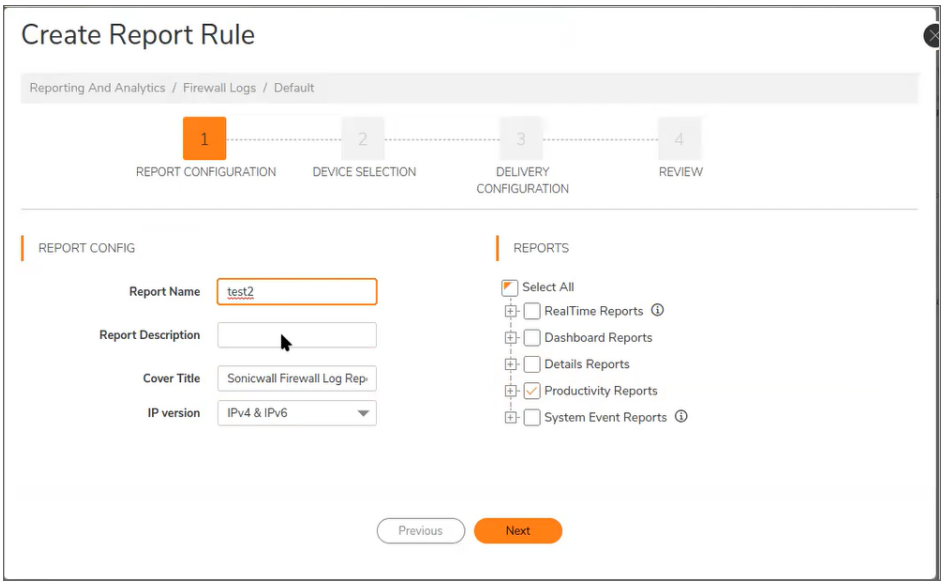
To set up a default report rule:

1. Click **Add** above the **Reports** table. Select the **Default** option and click **Next** to go to the **Report Configuration** page.

   ⓘ | **NOTE:** The below creation of Report Rule is from Manager View.



2. Fill the following details in the **Report Configuration** page and click **Next**.
   - **Firewall Name** - It will be the same firewall which you have selected and cannot be edited.
   - **Report Name** - Enter a name for the report.
   - **Report Description** - Enter a description for the report.
   - **IP Version** - Select **IPv4**, **IPv6** or **Both**.
   - **Reports** - Select **RealTime Reports, Dashboard Reports, Details Reports** or **Productivity Reports** based on your preference. You can also choose all of them by clicking Select All.



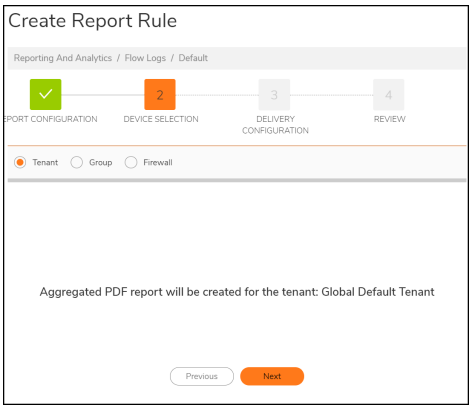
3. In the Device Selection screen, choose Tenant, Group or Firewall by clicking the radio button. The aggregated report is downloaded as a PDF.

   Tenant - When selected Tenant, it downloads information of all the tenants.

   Group - When selected Group, choose the groups from the list and click **Next**.

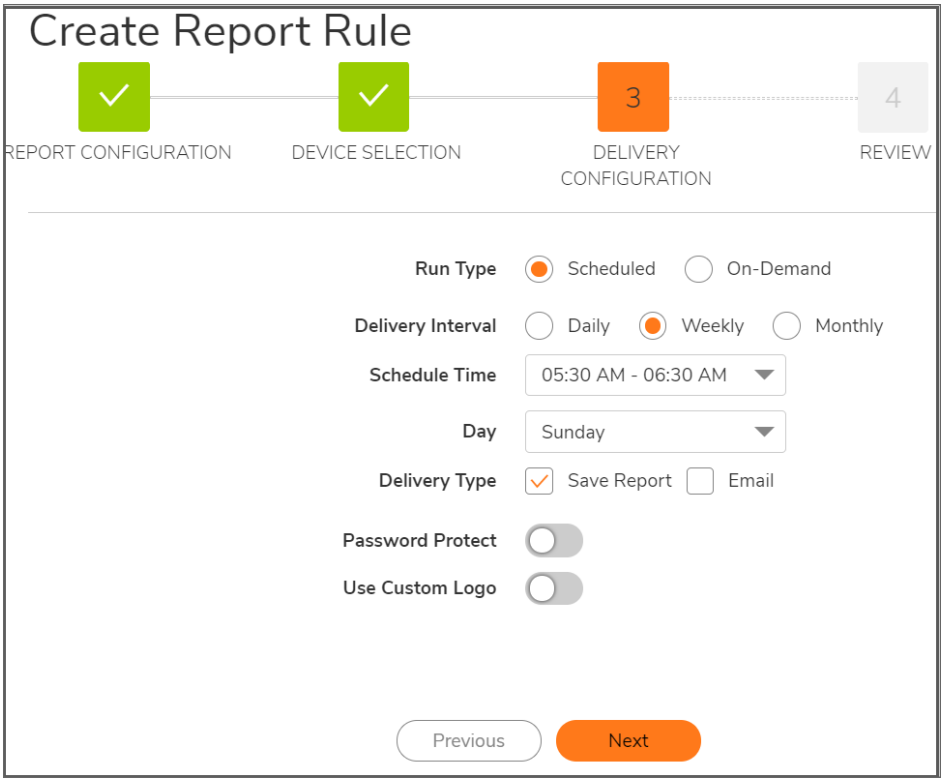
   Firewall - When selected Firewall, you can choose the individual firewalls or toggle the button to Aggregated report. Aggregated report contains the combined data of the selected devices. A maximum of 5 devices can be selected for aggregated report.

   ⓘ | **NOTE:** This screen doesn't appear if you are creating from Firewall view.

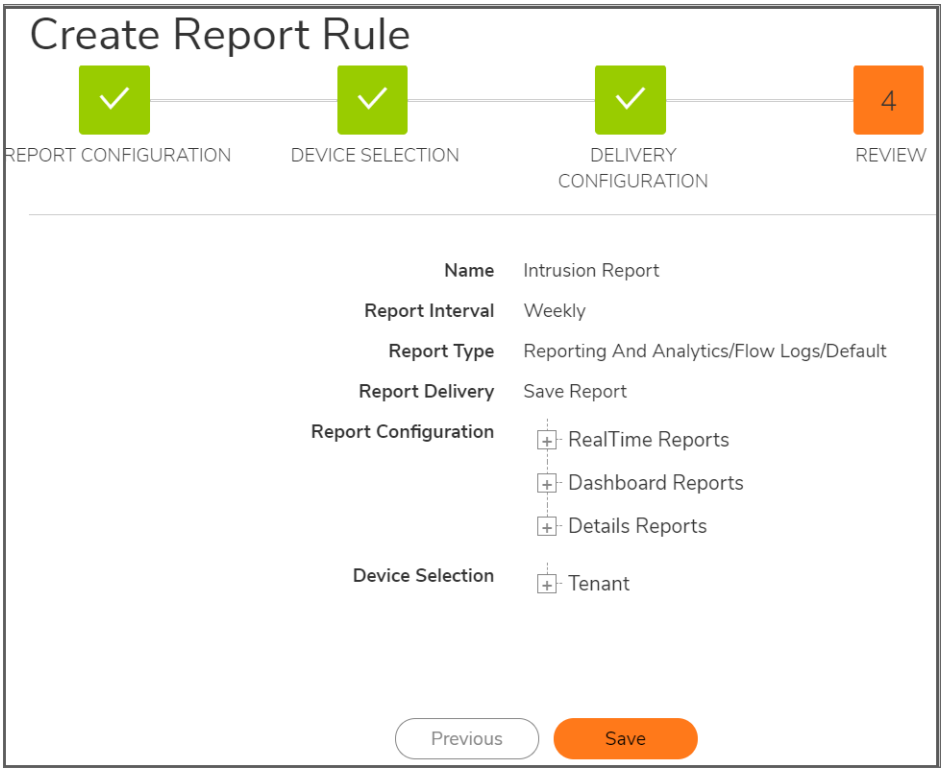


4. On the Delivery Configuration page fill the following information and click **Next**.
    - **On-demand Run Type** - It is used to change the time period of the report using the slider. The maximum report time permissible is 30 days.
    - **Scheduled Run Type** - It is used to choose when the report will be generated for a day, or for selected day of week or selected day of a month.
    - **Delivery Type** - You can select from **Save Report** and **Email** option. Save Report allows you to save the reports in NSM. You can view these saved report in NSM under **Reports > Saved Reports**. Email option allows you to email the report. To email the report you need to select the **Email Destination** as Administrator or Adhoc user. You need to provide the user mail id in the **Email Id** column if you select Adhoc User. You also need to add the **Email Subject** and **Body** as well as select **Zip Report** to send the report in a Zip format.
    - **Password Protect** - You can provide a password to the report pdf.

- **Use Custom Logo** - Upload a customized image for the logo.



5. On the **Review** page, you can review the data before generating the report. Click **Save** to confirm.



After you click on save, a new default rule is created on the **Report Rules** page with your report name.

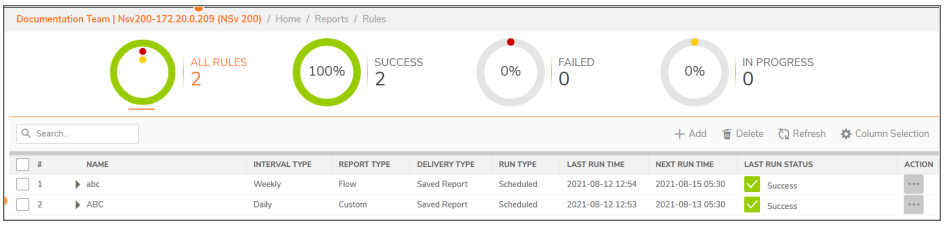
Firewall Up-Time Summary Report Rules

The **Firewall Up-Time Summary Report Rules** section provides the tools to manage the firewall up time report rules and view the reports once generated.

ⓘ **NOTE:** You can view and manage the Firewall Up-Time Summary Reports with both **NSM Advanced** and **NSM Essential** License.

Navigating the Firewall Up-Time Summary Report Rules Page

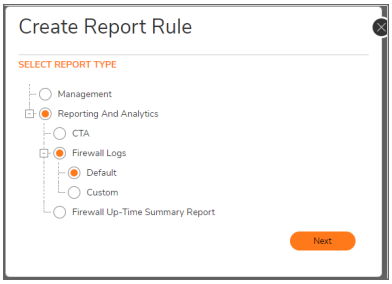
Go to **Reports > Rules** to view a list of all the reports that have been defined. The details of each report are shown in the table.



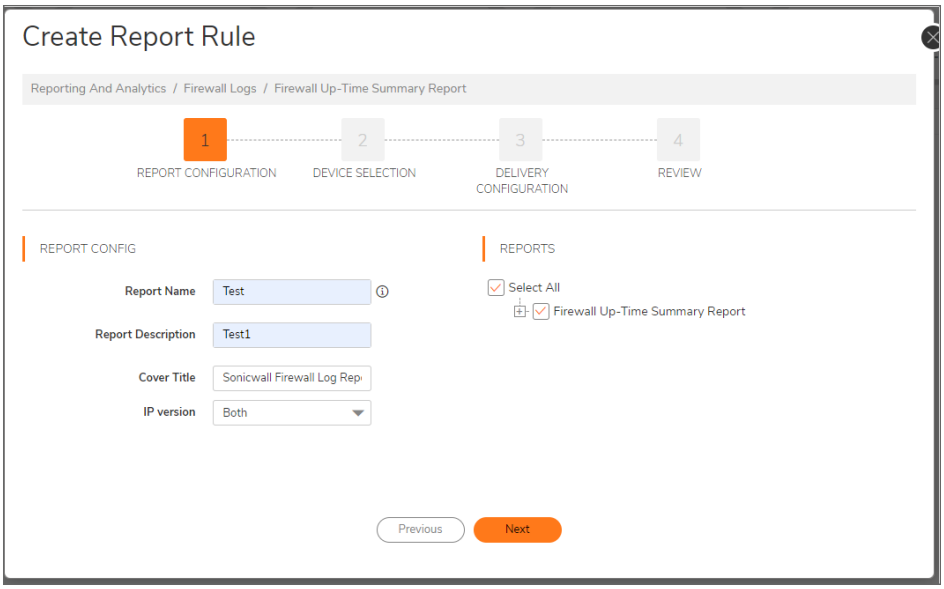
Setting Up the Firewall Up-Time Summary Report Rule

To set up a Firewall Up-Time Summary report rule:

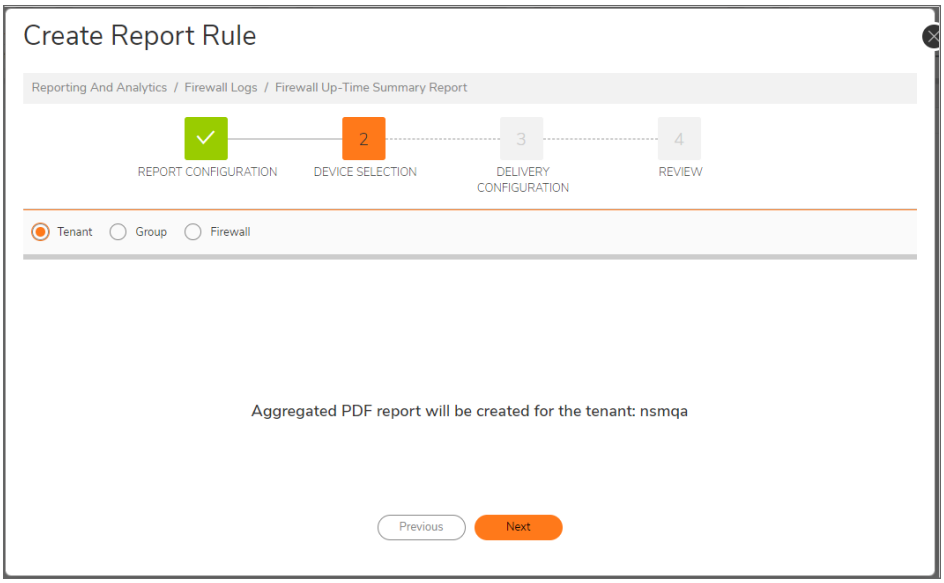
1. Click **Add** above the **Reports** table. Select the **Firewall Up-Time Summary Report** option and click **Next** to go to the **Report Configuration** page.



2. Fill the following details in the **Report Configuration** page and click **Next**.
   - **Report Name** - Enter a name for the report.
   - **Report Description** - Enter a description for the report.
   - **Cover Title** - Enter a cover title for the report.
   - **IP Version** - Select **IPv4**, **IPv6** or **Both**.
   - **Reports** - Select **Firewall Up-Time Summary Report**.



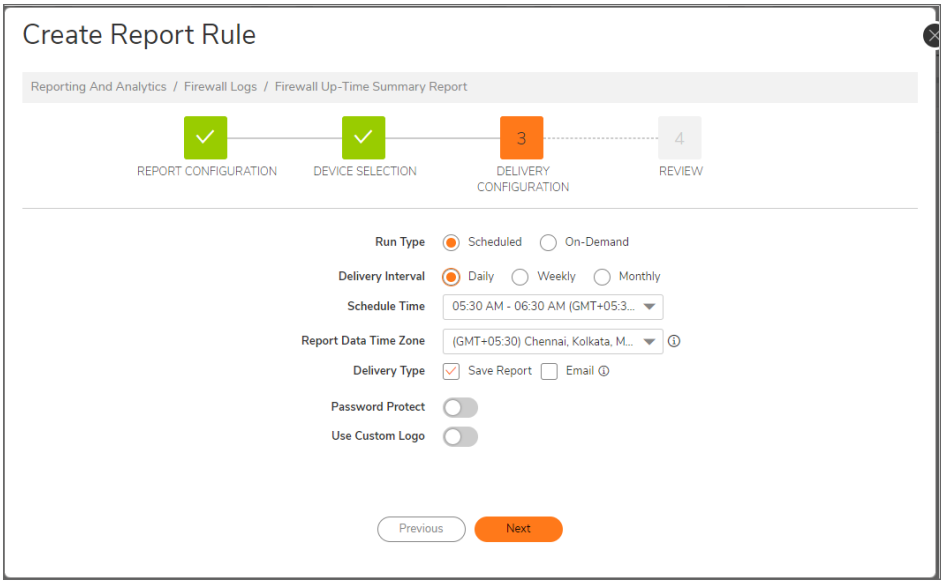
3. On the Device Selection page select from Tenant, Group or Firewall options.



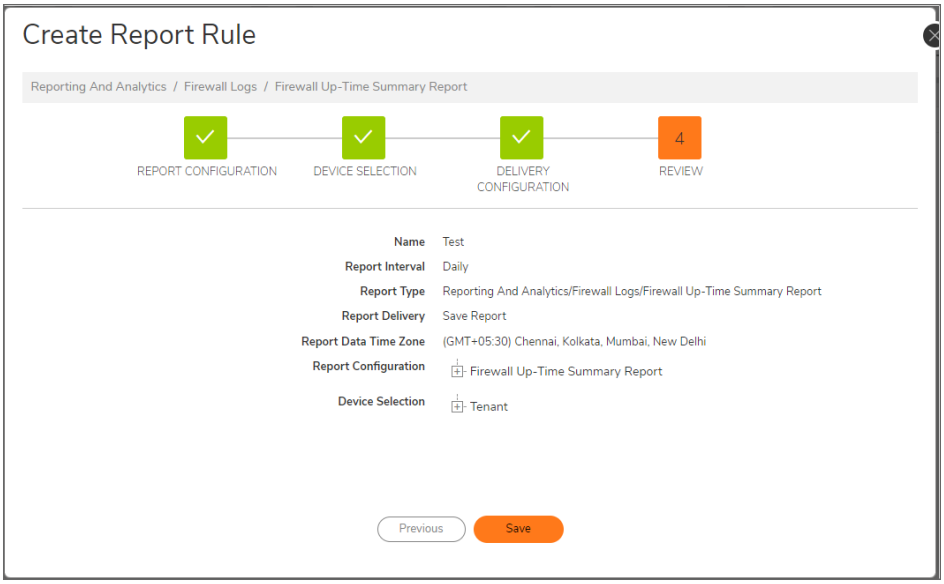
4. On the Delivery Configuration page fill the following information and click **Next**.
   - **On-demand Run Type** - It is used to change the time period of the report using the slider. The maximum report time permissible is 30 days.
   - **Scheduled Run Type** - It is used to choose when the report will be generated for a day, or for selected day of week or selected day of a month.
   - **Delivery Type** - You can select from **Save Report** and **Email** option. Save Report allows you to save the reports in NSM. You can view these saved report in NSM under **Reports > Saved Reports**. Email option allows you to email the report. To email the report you need to select the

Email Destination as Administrator or Adhoc user. You need to provide the user mail id in the **Email Id** column if you select Adhoc User. You also need to add the **Email Subject** and **Body** as well as select **Zip Report** to send the report in a Zip format.

- **Password Protect** - You can provide a password to the report pdf.
- **Use Custom Logo** - Upload a customized image for the logo.



5. On the **Review** page, you can review the data before generating the report. Click **Save** to confirm.



After you click on save, a new Firewall Up-Time Summary Report rule is created on the **Report Rules** page with your report name.

Custom Reports

The **Custom Reports** section provides the tool to produce customized reports and view them once generated. These reports can be customized by a user according to the collected data. The user can create custom filters or use the default filters to create these reports.

ⓘ | **NOTE:** You need to have NSM advance license to view and manage the Custom Reports.

ⓘ | **NOTE:** Custom reports can be generated in the **Reports** section of **Manager View** as well as **Firewall View.**

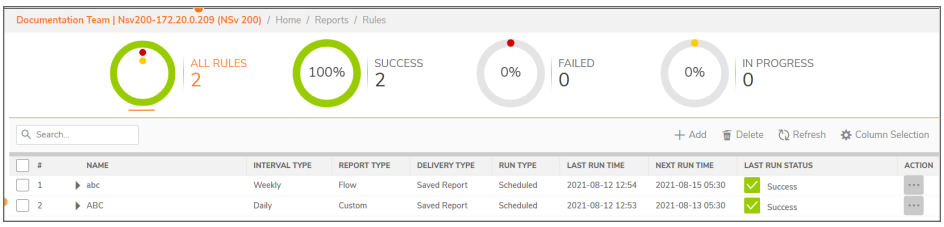
Creating Custom Filters

Before creating a custom report, an user first needs to create a custom filter as per their requirement. To learn more about creating custom filters you can check the Custom Filters section in the **Analytics** chapter.

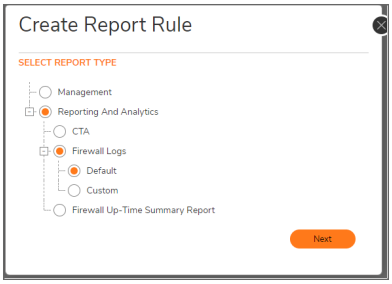
Navigating the Custom Reports Page

You can view the **Custom Report** section by navigating through the **Firewall View** or **Manager View** page. You will also be directed to this page automatically from the session log page by clicking on **Save and Create Report Rule**.

Go to **Report > Rules** section to view the report rules table.



Click on **Add** button to open the **Create Report Rule** dialog box. Select the **Custom** option and click **Next** to go to the **Basic Info** page.

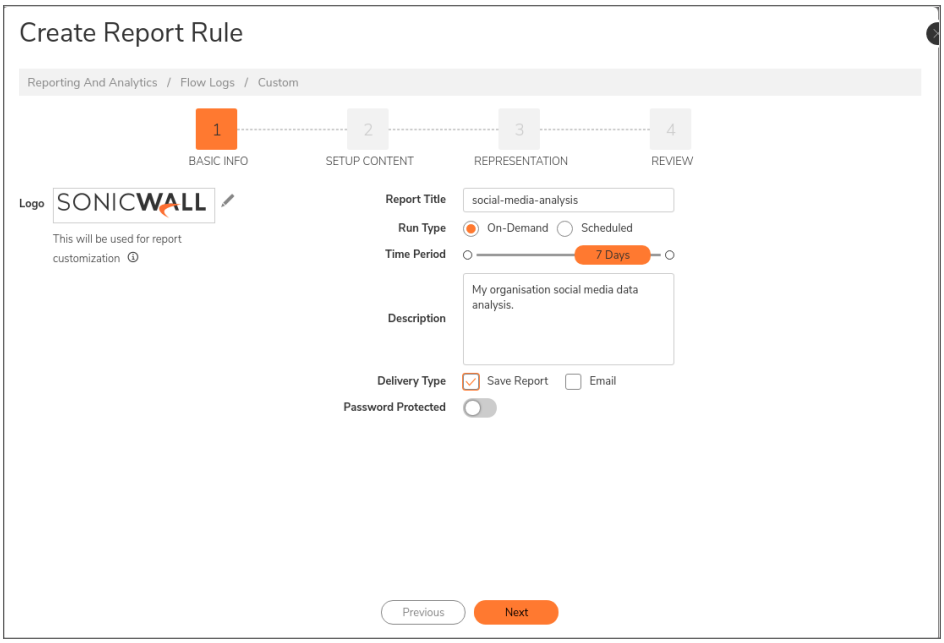


Basic Info

Basic Info page allows you to provide all the basic information for your report.

- **Logo** - This option allows you to add a custom logo to the report. You can only select a PNG format file having a maximum height of 160px and maximum width of 200px.
- **Report Title** - You can add a title to the report.
- **On-demand Run Type** - It is used to change the time period of the report using the slider. The maximum report time permissible is 30 days.
- **Scheduled Run Type** - It is used to choose when the report will be generated for a day, or for selected day of week or selected day of a month.
- **Description** - You can add a description to your report.
- **Delivery Type** - You can select from **Save Report** and **Email** option. Save Report allows you to save the reports in NSM. You can view these saved report in NSM under **Reports > Saved Reports**. Email option allows you to email the report. To email the report you need to select the **Email Destination** as Administrator or Adhoc user. You need to provide the user mail id in the **Email Id** column if you select Adhoc User. You also need to add the **Email Subject** and **Body** as well as select **Zip Report** to send the report in a Zip format.
- **Password Protect** - You can provide a password to the report pdf.

Click **Next** after filling all the required details.

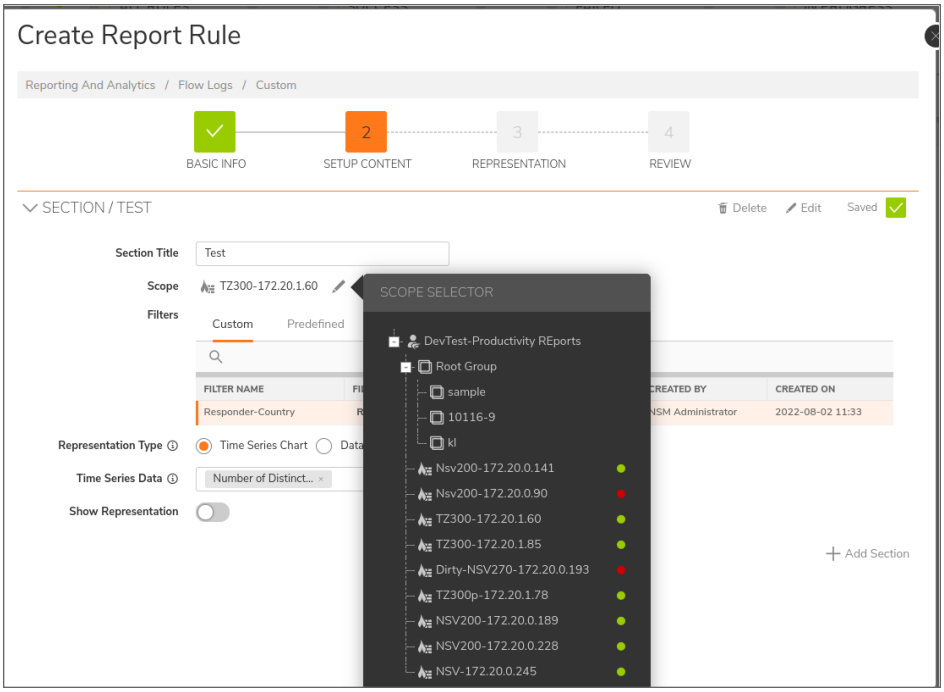


Setup Content

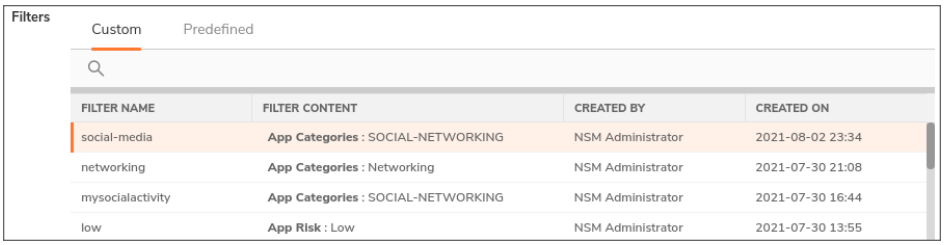
After filling the basic information, you will be directed to the **Setup Content** page. You need to fill the following details and click **Next**.

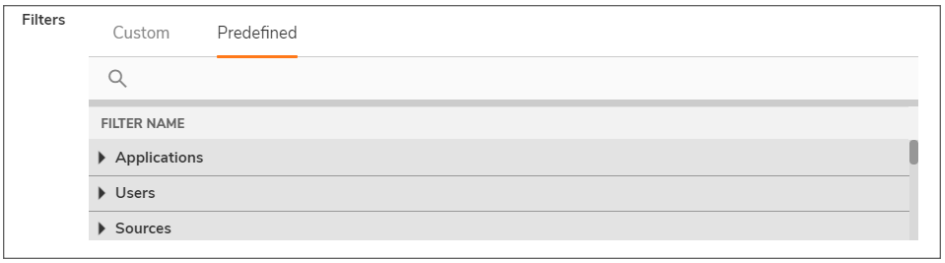
- **Section Title -** You can add a title to the report section.
- **Scope Selector -** You can change the scope of the report to any tenant or group level.

  ⓘ **NOTE:** The scope selector option is only available on custom reports for the Manager View and not the Firewall View.



- **Filters -** You can select from the list of **Custom Filters** that you have created or from a list of **Predefined** filters.



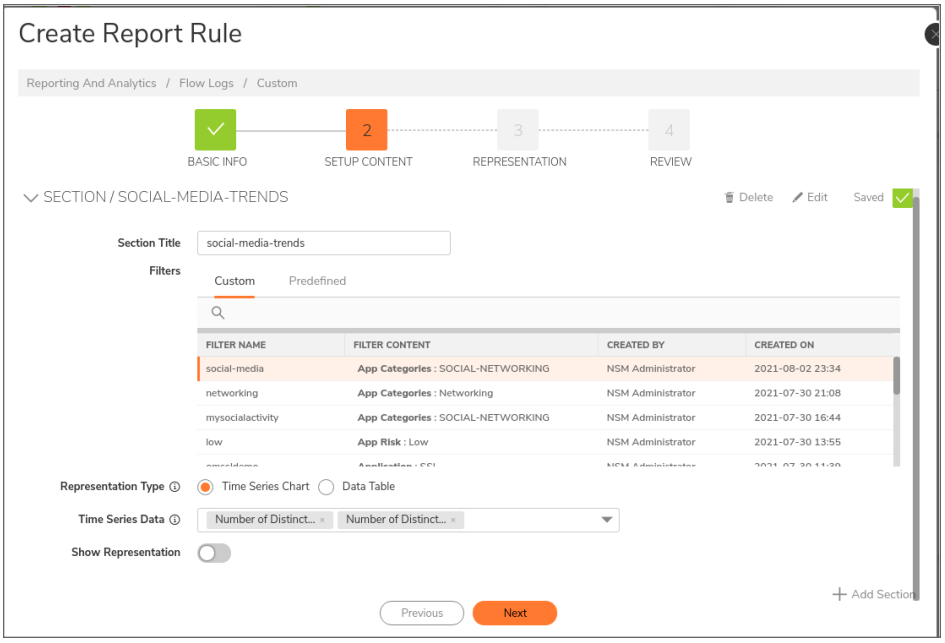


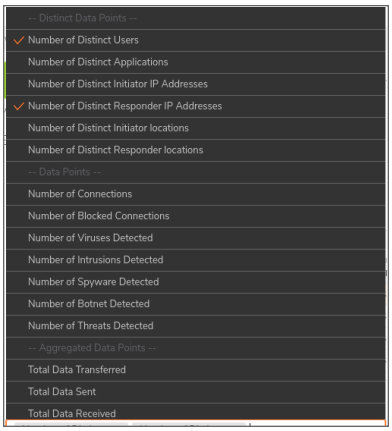
- **Representation Types -** You can select from **Time Series Chart** and **Data Table** option.

  Time Series Chart: This allows you to generate a report where the selected item values will be plotted in a time series chart. Each point on the chart corresponds to the number of data points of selected item(s) at a time-point. You can use the drop down to select your data points. The data points are divided into 3 different categories i.e. Distinct Data Points, Data Points and Aggregate Data Points.

  General recommendations:

  - Select an item that is not part of a filter criterion.
  - Select items for which y-axis magnitude is comparable, or create separate charts with different y-axis scales.

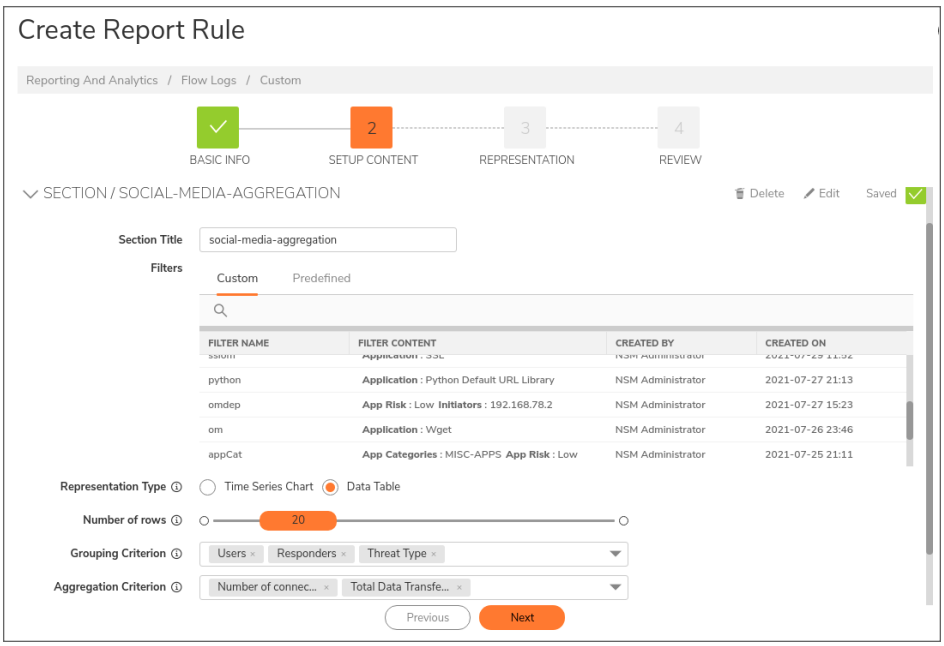




Data Table: This allows you to generate a report where the selected item values will be represented in a tabular manner. You have to make the appropriate selections from the list of **Grouping Criterion** and **Aggregated Criterion** to get the desired report. For example, you want a weekly report of users accessing high risk application where along with user name you need total number of connections, data send, total data transferred and total threat. To generate this report, you need to create custom filter to filter out all high risk applications and use data table custom report to generate the desired report..

You can also choose the **Number of Rows** of data that you want in the report.

ⓘ | **NOTE:** You can select from a maximum of 6 columns from the Grouping Criterion and Aggregated Criterion list.



- **Show representation -** This lets you see a representation of the report that you will generate according to your selections. Kindly note that this is only a representation and not the real data.

ⓘ | **NOTE:** You can click on **Add Section** to add multiple sections of information in your report.

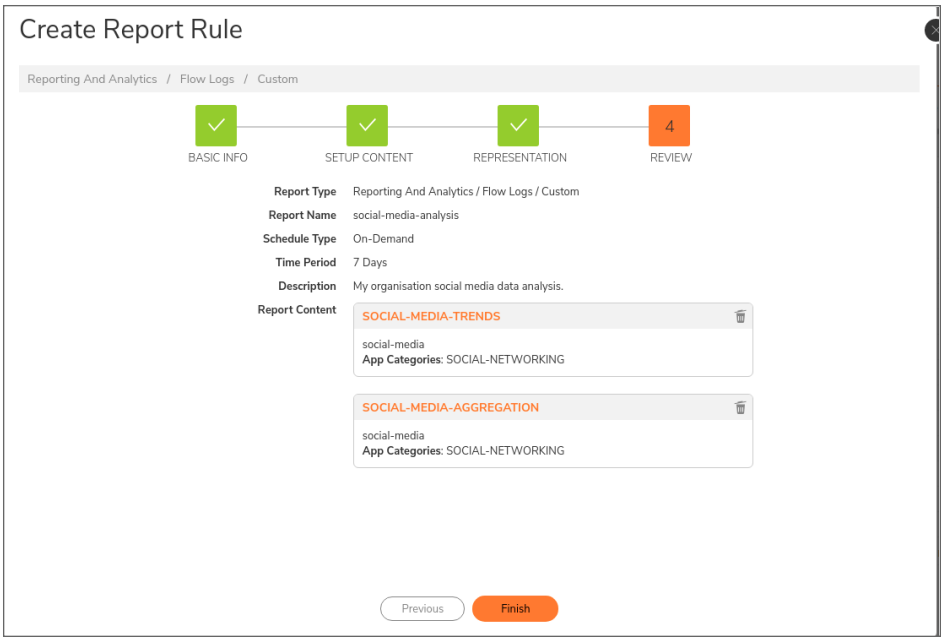
ⓘ | **NOTE:** You can **Delete** and **Edit** a section by clicking on the delete and edit symbol above a section.

Representation

This page provides you a representation of the data that will appear in your report as per the selections that you have made. The data is generated in the form of charts and tables along with the respective section title. You can drag and drop the section titles to rearrange them as per your requirement. Kindly note that this is not the real data. Click on **Next** to go to the Review page.

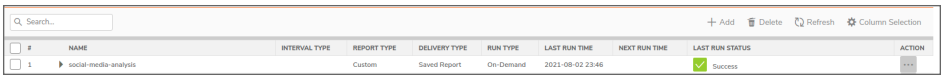
Review

The Review page lets you see all the information that your have added for your report. This provides you the opportunity to review the data before generating the report. Click on **Save** to save the custom report rule.



Generating and Downloading the Report

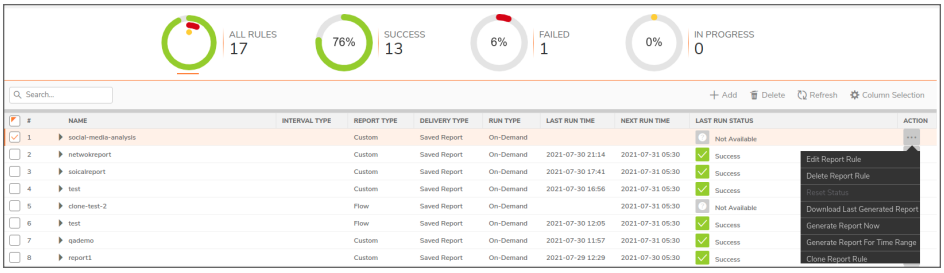
After you click on finish, a new rule is created on the **Report Rules** page with your report title. You can use the options provided to edit, delete, generate and download the report.



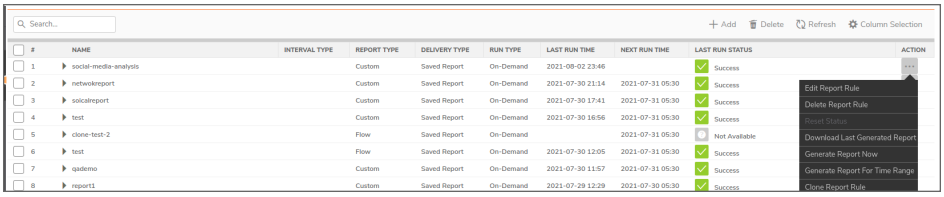
To generate and download a report:

1. Click on the three dots at the right of the report and select **Generate Report** Now. You can also select **Generate Report for Time Range** to generate the report for a selected time range. Click on **Refresh** to

refresh the data.



2. Once the report is generated successfully, click on the three dots at the right of the report and select **Download Last Generated Report** to download the report to your system in a pdf format. You can open the pdf to view the generated report.



ⓘ **NOTE:** You can Edit or Delete an existing report rule by clicking on the **Edit Report Rule** or **Delete Report Rule** button.

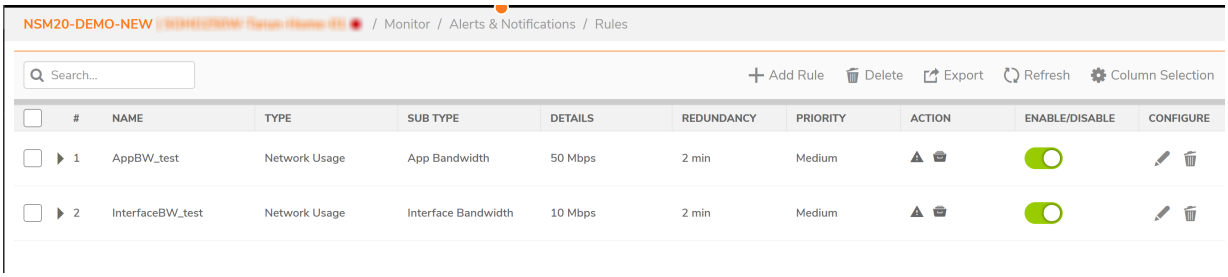
ⓘ **NOTE:** You can create another report rule using the properties of an existing report rule by clicking on the **Clone Report** button.

ⓘ **NOTE:** You can reset a currently running task for a selected rule using the **Reset Status** button.

Alerts and Notifications

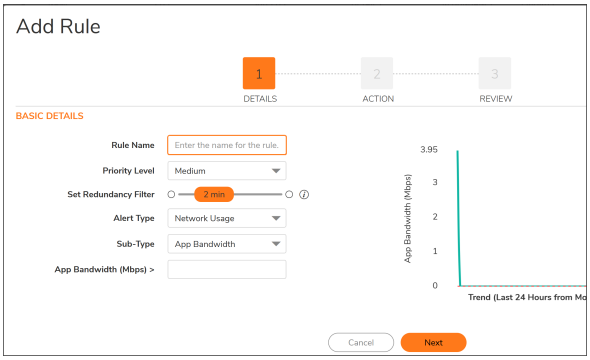
Rules

Using Alerts, you can create rules for the notices and see historic alerts and notifications for the following alert types: Network Usage, Threat, Web Activities, Geo-Location, and System Events. You can set how you want to receive notifications when a type of alert is created. You can choose to get alerts in Notification Center, receive emails, and save notifications when an alert is triggered.



Creating an alert rule:

1. In **FIREWALL VIEW**, select **MONITOR**
2. Click **Rules**.
3. Click **Add Rule**.

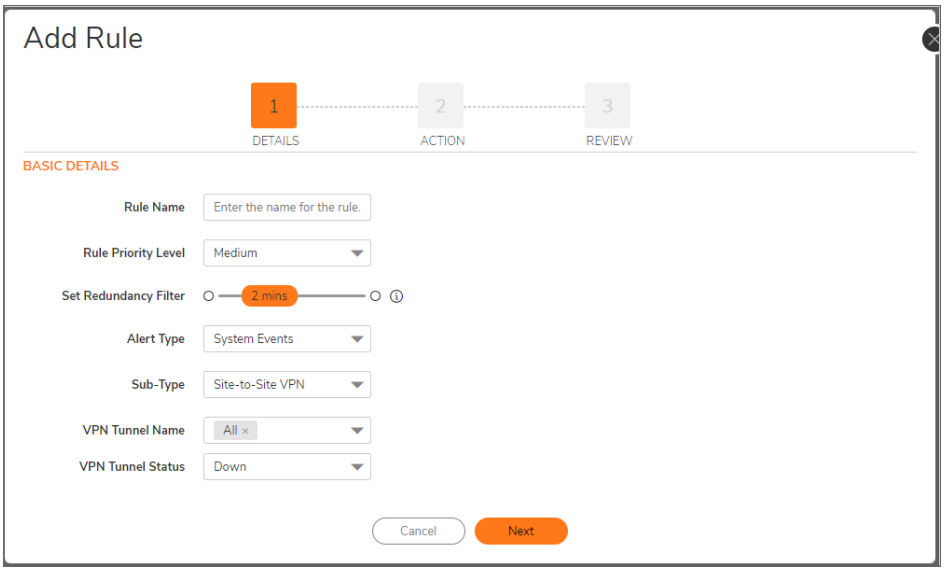


4. Enter a name and select Priority level.
5. Set **Redundancy Filter.**
6. Select the **Alert Type**.
7. Select alert **Sub-Type** and enter app bandwidth in Mbps.
8. Click **Next**.
9. In the Actions page, select how you want to be alerted for the rule. The options are System Alerts, Email.
10. Select the History options to save the alerts if required.
11. Click **Next**.
12. Review the rule and click **Save**.

VPN Tunnel Status Alert

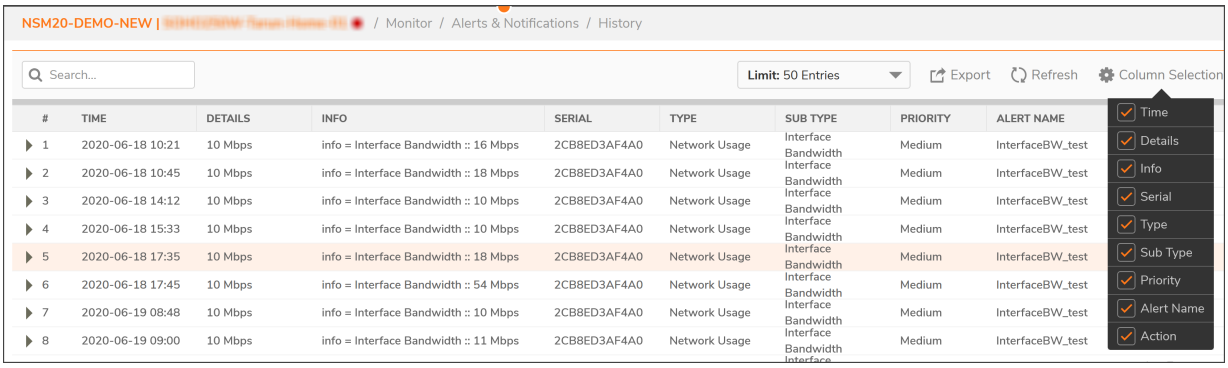
VPN tunnel status alert is now available from NSM SaaS **2.3.5** onwards for both **GEN6** and **GEN 7** firewalls. You can refer the Release Notes to learn more about the latest build information. This feature requires the flow log transport mechanism to be changed to encrypted mode.

To enable this alert you need to create a new alert rule and select the Alert Type as **System Events** and the Sub-Type as **Site-to-Site VPN**. You also need to enter the **VPN Tunnel Name** and VPN **Tunnel Status** from the drop-down list.



History

The **History** feature shows the historic alerts generated for the rules you have created. The historic alert report can be customized based on time, details, info, type, sub-type, priority, alert name, and action. You can export the report as a CSV file for archiving purposes.



#	TIME	DETAILS	INFO	SERIAL	TYPE	SUB TYPE	PRIORITY	ALERT NAME
1	2020-06-18 10:21	10 Mbps	info = Interface Bandwidth :: 16 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test
2	2020-06-18 10:45	10 Mbps	info = Interface Bandwidth :: 18 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test
3	2020-06-18 14:12	10 Mbps	info = Interface Bandwidth :: 10 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test
4	2020-06-18 15:33	10 Mbps	info = Interface Bandwidth :: 10 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test
5	2020-06-18 17:35	10 Mbps	info = Interface Bandwidth :: 18 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test
6	2020-06-18 17:45	10 Mbps	info = Interface Bandwidth :: 54 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test
7	2020-06-19 08:48	10 Mbps	info = Interface Bandwidth :: 10 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test
8	2020-06-19 09:00	10 Mbps	info = Interface Bandwidth :: 11 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test

To export historic alerts:

1. Click the **Export** icon.
2. In the **Export to File** dialog, click **OK**.
3. Save file to local machine.

10

Logs

The **Logs** section provides the tools to view the system logs, authentication logs and auditing logs as well as download the logs in CSV format. Firewall logs can be used by the administrator for troubleshooting network. You can access the system logs by navigating to **System Logs** under the **Logs** tab on the **Monitor View** of a firewall.

Topics:

- System Logs
- Authentication Logs
- Auditing Logs

System Logs

You need to have the following pre-requisites to view and manage System Logs:

- System logs are available for both **GEN6** and **GEN 7** firewalls.
- You can enable System logs for devices with lower version of Sonic OS by upgrading the firmware. You can refer to Enabling System Logs for Existing Firewalls to see more details.
- System logs archival are supported for 30 days.
- You can refer to the System Events Reference Guide to see the list of default system logs that are supported for NSM SaaS.

ⓘ | **NOTE:** You need to have **NSM Advance License** to view and manage System Logs.

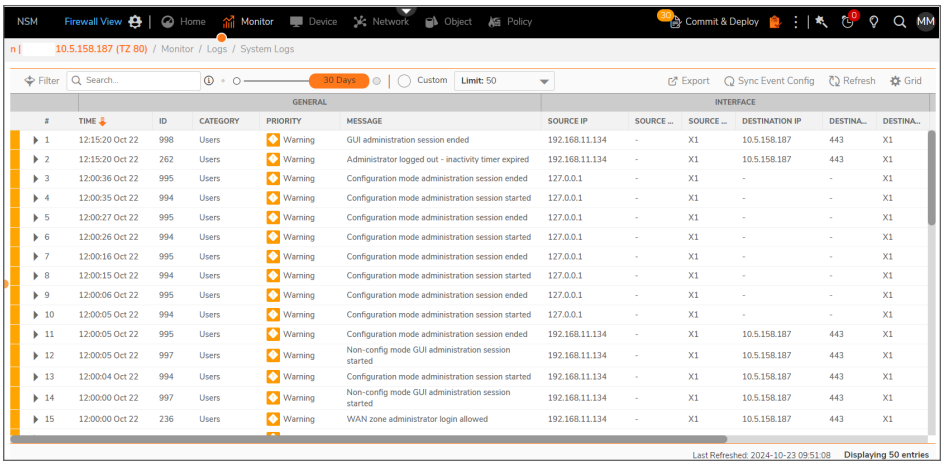
Navigating to System Logs Page

To see the list of logs that have been created click on **System Logs** page on the **Monitor View** of the firewall. You can use the **Search** option to search for a particular log.

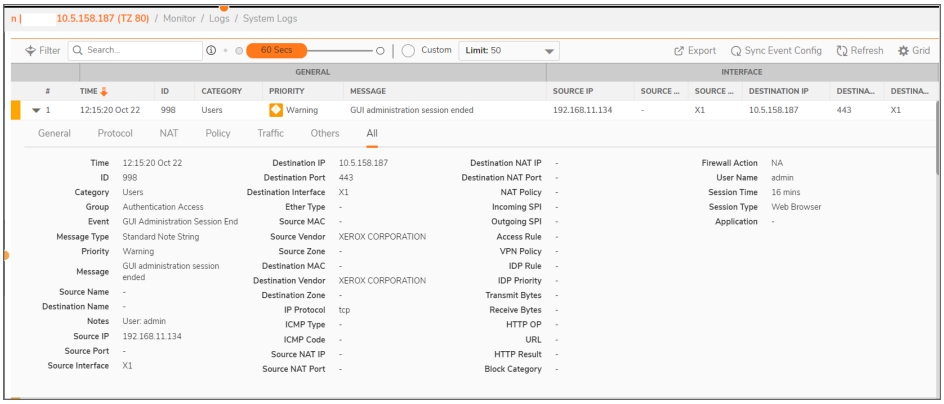
You have a **Time Range** option that lets you customize the time duration of the report. The **Limit** drop down is used to set the limit of the number of displayed logs. You can further filter the graph according to a specific time by using the **Time Slider** which is present above the graph.

You can also click on **Refresh** button to refresh the information on the page and export the table in CSV format using the **Export** button. The columns of the table can be edited using the **Grid Settings** button at the top of the page.

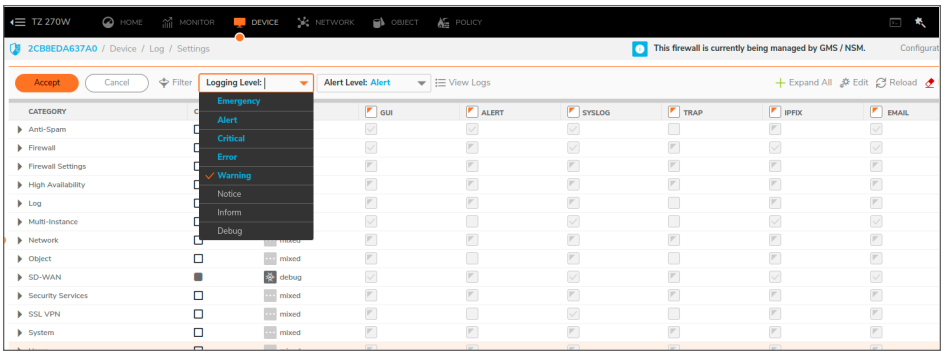
The logs categories in the list have been color coded which can be viewed on the extreme left column.

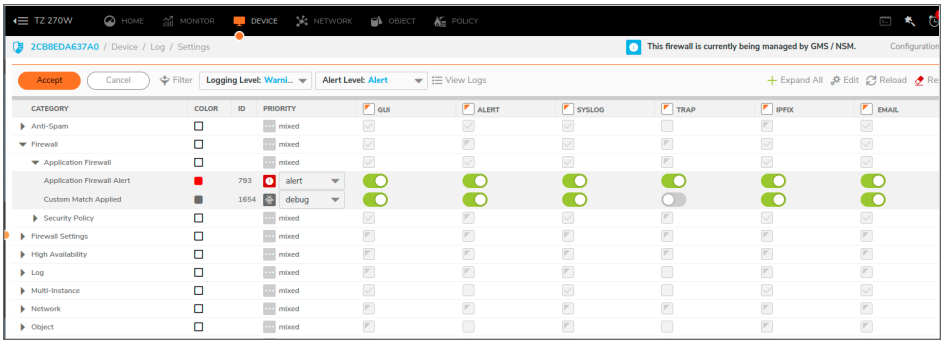


You can expand each of the logs to see additional information such as event ID, category, event name, message, priority, source IP, destination IP etc.



Only the following **Priority** levels for System Logs are supported for egressing to NSM SaaS - Alerts, Critical, Error, and Warning. For a log priority to show up in NSM SaaS, its IPFIX setting has to be enabled on the **Log>Settings** page of the **Device View**.

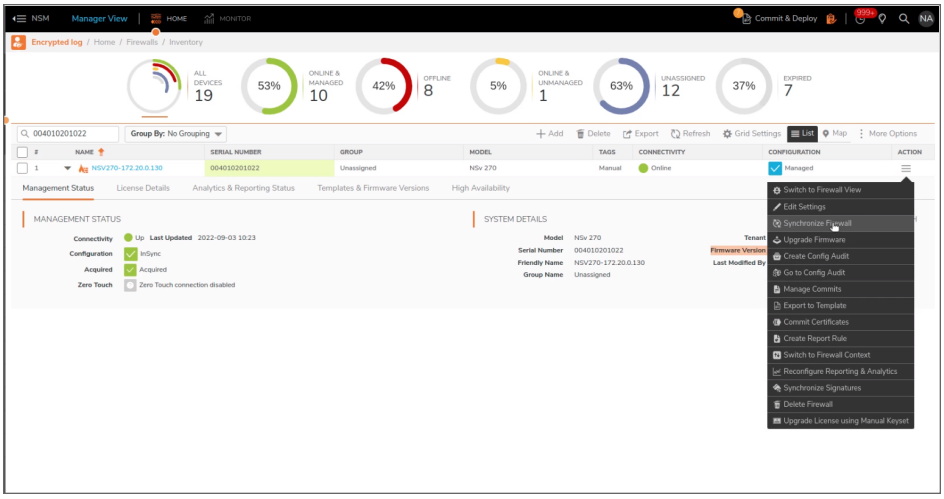




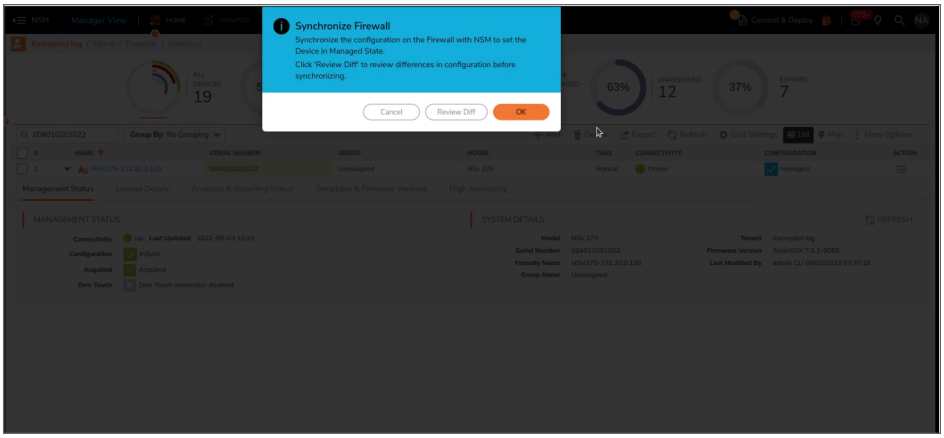
Enabling System Logs for Existing Firewalls

If your device has a lower firmware version then you can enable **System Logs** by first upgrading your firmware. You can refer to the NSM Administration Guide to upgrade your firmware. Next, you need to follow the steps given below. This applicable for both GEN6 and GEN7 firewalls:

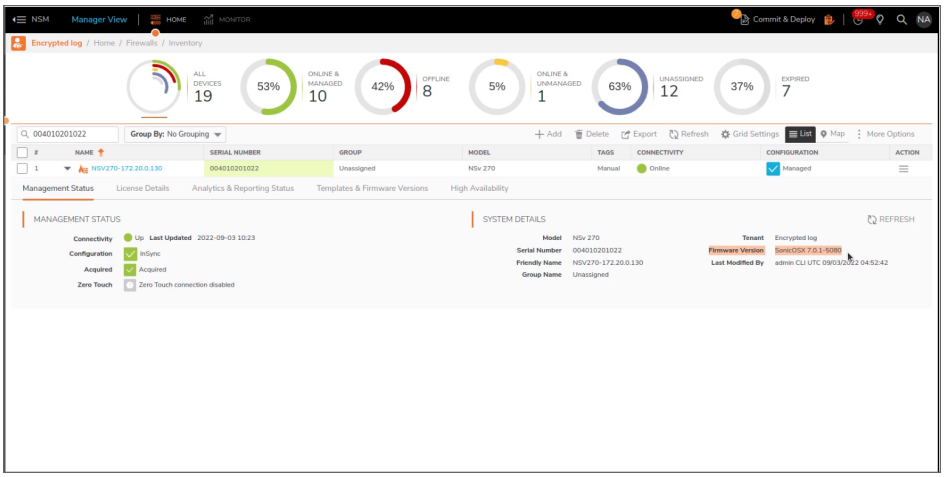
1. Click on **Synchronize Firewall** option under **Actions** on the **Firewall > Inventory** page.



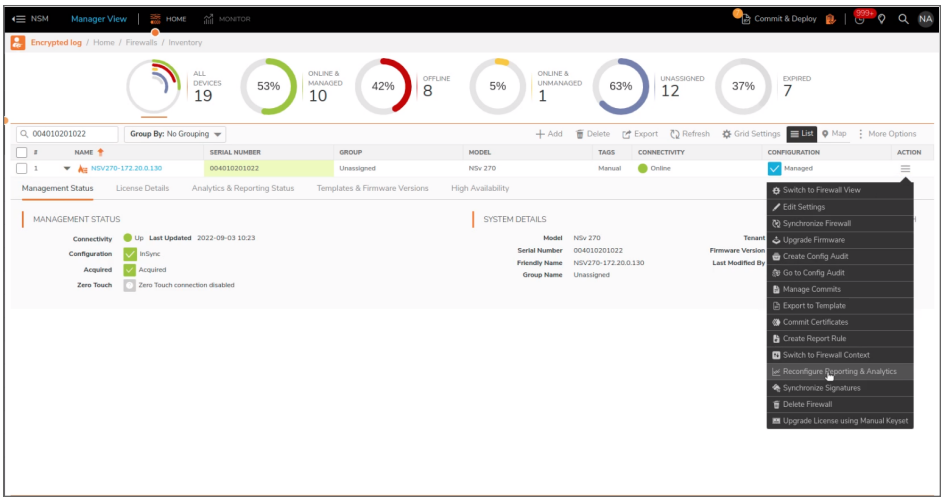
2. Click on **OK** to complete the synchronization.



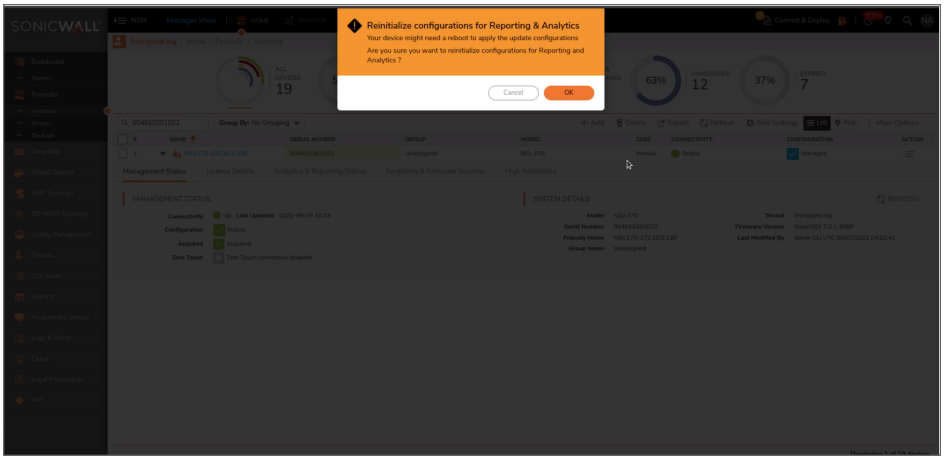
3. You can view the **Firmware Version** under the firewall to confirm if the updated version is appearing on the firewall.



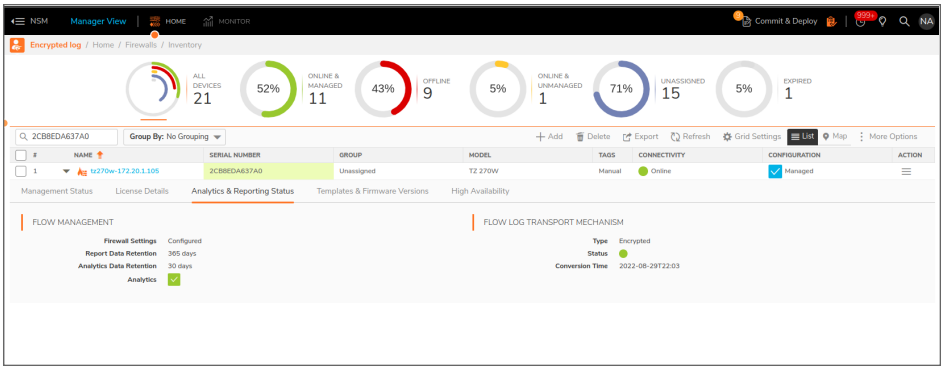
4. Next, click on **Reconfigure Reporting and Analytics** option under **Actions** on the **Firewall > Inventory** page.



5. Click on **OK** to complete the reconfiguration.



6. After the reporting and analytics is reconfigured, check if the flow log transport mechanism has changed from VPN to Encrypted mode. If it is changed successfully, the system will disable the SGMSServer-VPN tunnel that is established to transfer flow logs to NSM and you should not enable this tunnel manually.



Once you have successfully completed all the steps, you will be able to view the **System Logs** option in the **Monitor View** of the firewall.

ⓘ | **NOTE:** There may be momentary loss of data in the firewall while reconfiguring reporting and analytics.

Authentication Logs

This section provides you with the tools to view and generate user authentication reports for user login/logout, admin login/logout and failed login reports. You can access the **Authentication Logs** by navigating under the **Logs** tab.

ⓘ | **NOTE:** You need to have **NSM Advance License** to view and manage Authentication Logs.

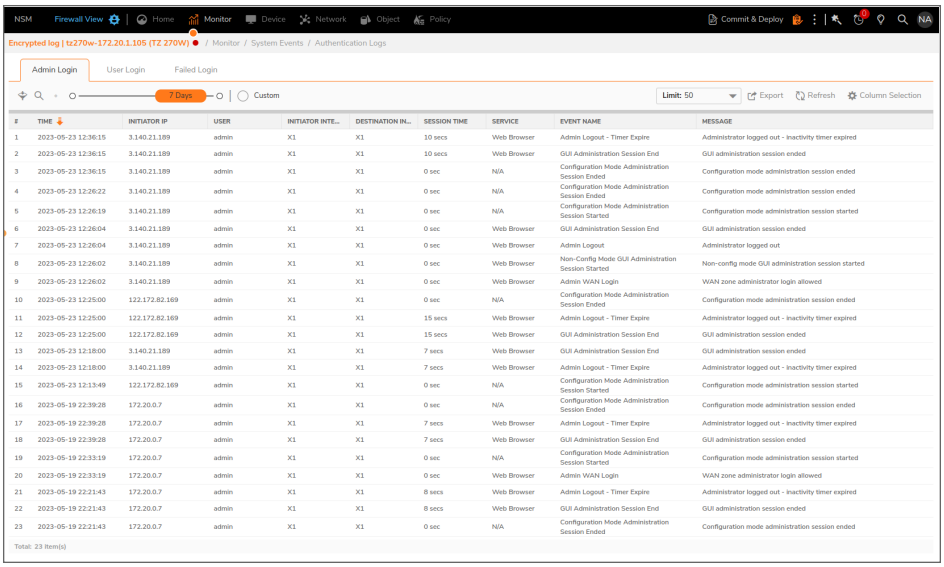
ⓘ | **NOTE:** Authentication Logs are available for both **GEN6** and **GEN 7** firewalls. You can refer the Release Notes to learn more about the build information.

- **User Login:** This tab provides all the login/logout information of the user.
- **Admin Login:** This tab provides all the login/logout information of the administrator of a firewall.
- **Failed Login:** This tab provides all the information regarding the failed login attempt of both the user and the administrator.
- The report column includes information such as Time, Initiator IP, User, Initiator/Destination Interface, Initiator/Destination Port, Session Time, Service and Message

You can use the **Search** button to search the information of an user. You have a **Time Range** option that lets you customize the time duration of the report. The **Limit** drop down is used to set the limit of the number of users. You can further filter the table according to a specific time by using the **Time Slider** which is present above the graph.

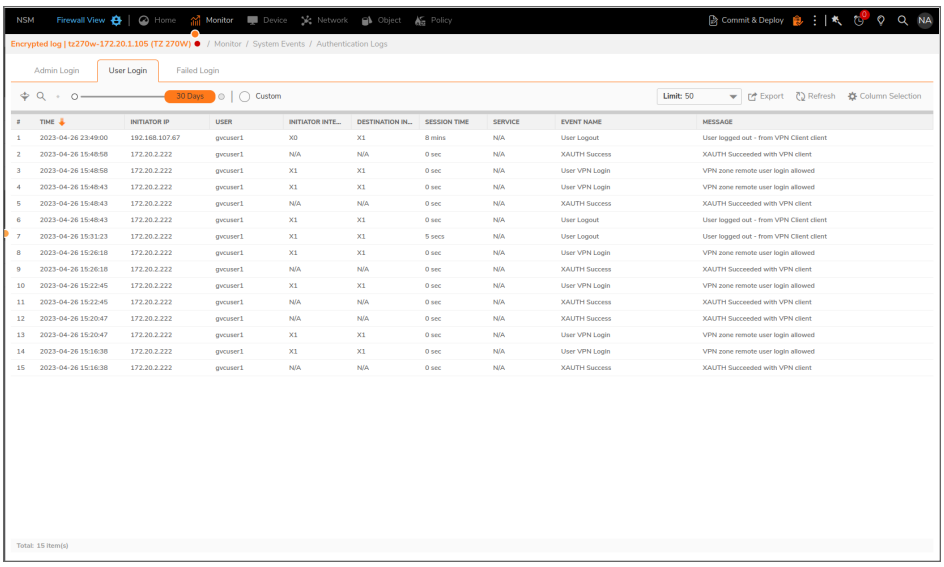
You have the option to create **Customized Filters** as per your requirements for the initiator IP and the user columns as well as create **Custom Reports**. You can also click on **Refresh** button to refresh the information on the page, edit the columns in the table by the **Column Selection** button and export the table in PDF/CSV format using the **Export** button.

Admin Login:



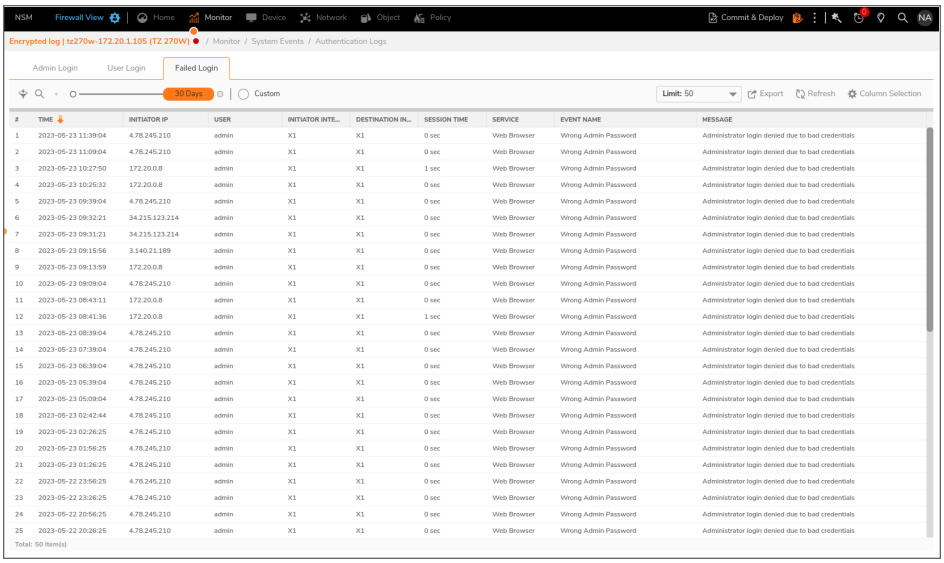
#	TIME	INITIATOR IP	USER	INITIATOR INTE...	DESTINATION IN...	SESSION TIME	SERVICE	EVENT NAME	MESSAGE
1	2023-05-23 12:36:15	3.140.21.189	admin	X1	X1	10 secs	Web Browser	Admin Logout - Timer Expire	Administrator logged out - inactivity timer expired
2	2023-05-23 12:36:15	3.140.21.189	admin	X1	X1	10 secs	Web Browser	GUI Administration Session End	GUI administration session ended
3	2023-05-23 12:36:15	3.140.21.189	admin	X1	X1	0 sec	N/A	Configuration Mode Administration Session Ended	Configuration mode administration session ended
4	2023-05-23 12:26:22	3.140.21.189	admin	X1	X1	0 sec	N/A	Configuration Mode Administration Session Ended	Configuration mode administration session ended
5	2023-05-23 12:26:19	3.140.21.189	admin	X1	X1	0 sec	N/A	Configuration Mode Administration Session Started	Configuration mode administration session started
6	2023-05-23 12:26:04	3.140.21.189	admin	X1	X1	0 sec	Web Browser	GUI Administration Session End	GUI administration session ended
7	2023-05-23 12:26:04	3.140.21.189	admin	X1	X1	0 sec	Web Browser	Admin Logout	Administrator logged out
8	2023-05-23 12:26:02	3.140.21.189	admin	X1	X1	0 sec	Web Browser	Non-Config Mode GUI Administration Session Started	Non-config mode GUI administration session started
9	2023-05-23 12:26:02	3.140.21.189	admin	X1	X1	0 sec	Web Browser	Admin WAN Login	WAN zone administrator login allowed
10	2023-05-23 12:25:00	122.172.82.169	admin	X1	X1	0 sec	N/A	Configuration Mode Administration Session Ended	Configuration mode administration session ended
11	2023-05-23 12:25:00	122.172.82.169	admin	X1	X1	15 secs	Web Browser	Admin Logout - Timer Expire	Administrator logged out - inactivity timer expired
12	2023-05-23 12:25:00	122.172.82.169	admin	X1	X1	15 secs	Web Browser	GUI Administration Session End	GUI administration session ended
13	2023-05-23 12:18:00	3.140.21.189	admin	X1	X1	7 secs	Web Browser	GUI Administration Session End	GUI administration session ended
14	2023-05-23 12:18:00	3.140.21.189	admin	X1	X1	7 secs	Web Browser	Admin Logout - Timer Expire	Administrator logged out - inactivity timer expired
15	2023-05-23 12:13:49	122.172.82.169	admin	X1	X1	0 sec	N/A	Configuration Mode Administration Session Started	Configuration mode administration session started
16	2023-05-19 22:39:28	172.20.0.7	admin	X1	X1	0 sec	N/A	Configuration Mode Administration Session Ended	Configuration mode administration session ended
17	2023-05-19 22:39:28	172.20.0.7	admin	X1	X1	7 secs	Web Browser	Admin Logout - Timer Expire	Administrator logged out - inactivity timer expired
18	2023-05-19 22:39:28	172.20.0.7	admin	X1	X1	7 secs	Web Browser	GUI Administration Session End	GUI administration session ended
19	2023-05-19 22:33:19	172.20.0.7	admin	X1	X1	0 sec	N/A	Configuration Mode Administration Session Started	Configuration mode administration session started
20	2023-05-19 22:33:19	172.20.0.7	admin	X1	X1	0 sec	Web Browser	Admin WAN Login	WAN zone administrator login allowed
21	2023-05-19 22:21:43	172.20.0.7	admin	X1	X1	8 secs	Web Browser	Admin Logout - Timer Expire	Administrator logged out - inactivity timer expired
22	2023-05-19 22:21:43	172.20.0.7	admin	X1	X1	8 secs	Web Browser	GUI Administration Session End	GUI administration session ended
23	2023-05-19 22:21:43	172.20.0.7	admin	X1	X1	0 sec	N/A	Configuration Mode Administration Session Ended	Configuration mode administration session ended

User Login:



#	TIME	INITIATOR IP	USER	INITIATOR INTE...	DESTINATION IN...	SESSION TIME	SERVICE	EVENT NAME	MESSAGE
1	2023-04-26 23:49:00	192.168.107.67	gvcuser1	X0	X1	8 mins	N/A	User Logout	User logged out - from VPN Client client
2	2023-04-26 15:48:58	172.20.2.222	gvcuser1	N/A	N/A	0 sec	N/A	XAUTH Success	XAUTH Succeeded with VPN client
3	2023-04-26 15:48:58	172.20.2.222	gvcuser1	X1	X1	0 sec	N/A	User VPN Login	VPN zone remote user login allowed
4	2023-04-26 15:48:43	172.20.2.222	gvcuser1	X1	X1	0 sec	N/A	User VPN Login	VPN zone remote user login allowed
5	2023-04-26 15:48:43	172.20.2.222	gvcuser1	N/A	N/A	0 sec	N/A	XAUTH Success	XAUTH Succeeded with VPN client
6	2023-04-26 15:48:43	172.20.2.222	gvcuser1	X1	X1	0 sec	N/A	User Logout	User logged out - from VPN Client client
7	2023-04-26 15:31:23	172.20.2.222	gvcuser1	X1	X1	5 secs	N/A	User Logout	User logged out - from VPN Client client
8	2023-04-26 15:26:18	172.20.2.222	gvcuser1	X1	X1	0 sec	N/A	User VPN Login	VPN zone remote user login allowed
9	2023-04-26 15:26:18	172.20.2.222	gvcuser1	N/A	N/A	0 sec	N/A	XAUTH Success	XAUTH Succeeded with VPN client
10	2023-04-26 15:22:45	172.20.2.222	gvcuser1	X1	X1	0 sec	N/A	User VPN Login	VPN zone remote user login allowed
11	2023-04-26 15:22:45	172.20.2.222	gvcuser1	N/A	N/A	0 sec	N/A	XAUTH Success	XAUTH Succeeded with VPN client
12	2023-04-26 15:20:47	172.20.2.222	gvcuser1	N/A	N/A	0 sec	N/A	XAUTH Success	XAUTH Succeeded with VPN client
13	2023-04-26 15:20:47	172.20.2.222	gvcuser1	X1	X1	0 sec	N/A	User VPN Login	VPN zone remote user login allowed
14	2023-04-26 15:16:38	172.20.2.222	gvcuser1	X1	X1	0 sec	N/A	User VPN Login	VPN zone remote user login allowed
15	2023-04-26 15:16:38	172.20.2.222	gvcuser1	N/A	N/A	0 sec	N/A	XAUTH Success	XAUTH Succeeded with VPN client

Failed Login:



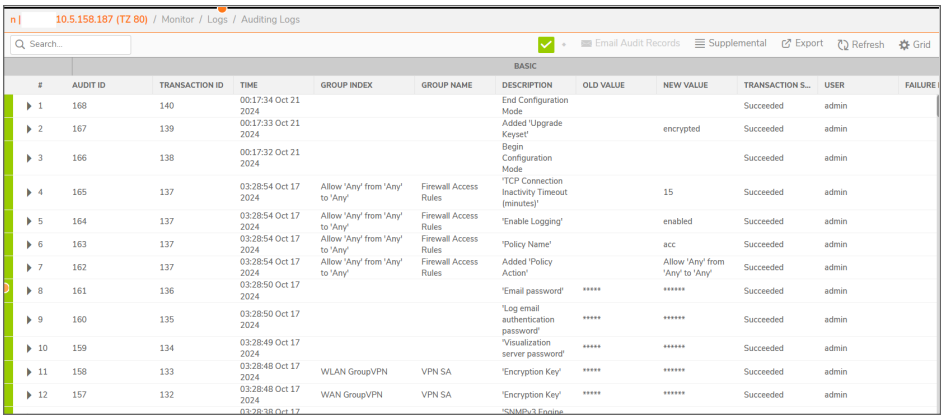
Auditing Logs

This section provides you with the tools to view and generate auditing log reports. Auditing logs fetch information from the firewall in real-time when the user clicks on the NSM auditing log menu and displays it in the NSM user interface. These logs are not stored in NSM. You can access the **Auditing Logs** by navigating under the **Logs** tab. The log data is available for **30 days**.

ⓘ | **NOTE:** You need to have **NSM Advance License** to view and manage Auditing Logs.

ⓘ | **NOTE:** Auditing Logs are available for both **GEN6** and **GEN 7** firewalls.

You can use the **Search** button to search the information of an user. You can also click on **Refresh** button to refresh the information on the page, edit the columns in the table by the **Grid** button and export the table in PDF/CSV format using the **Export** button.

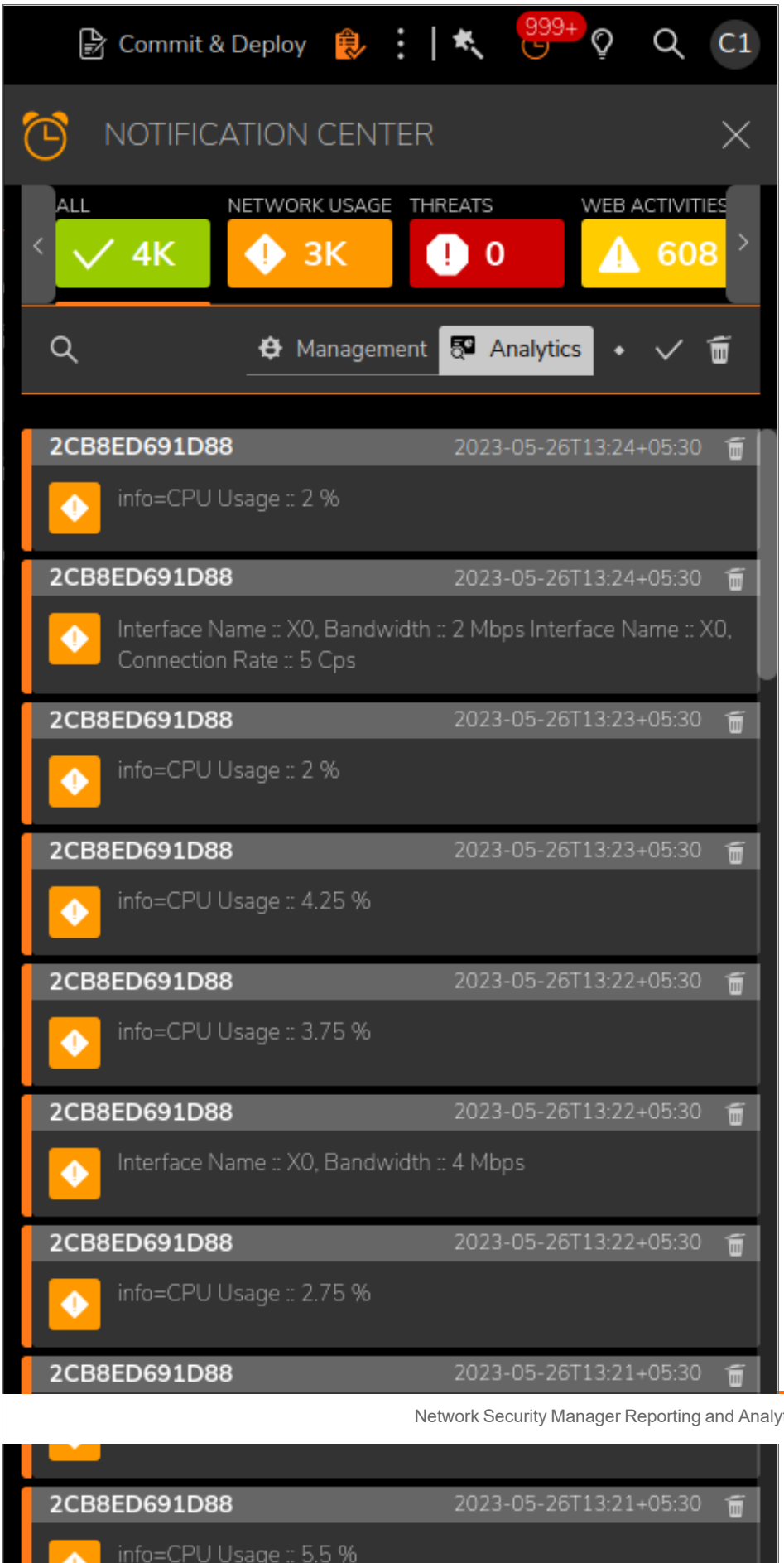


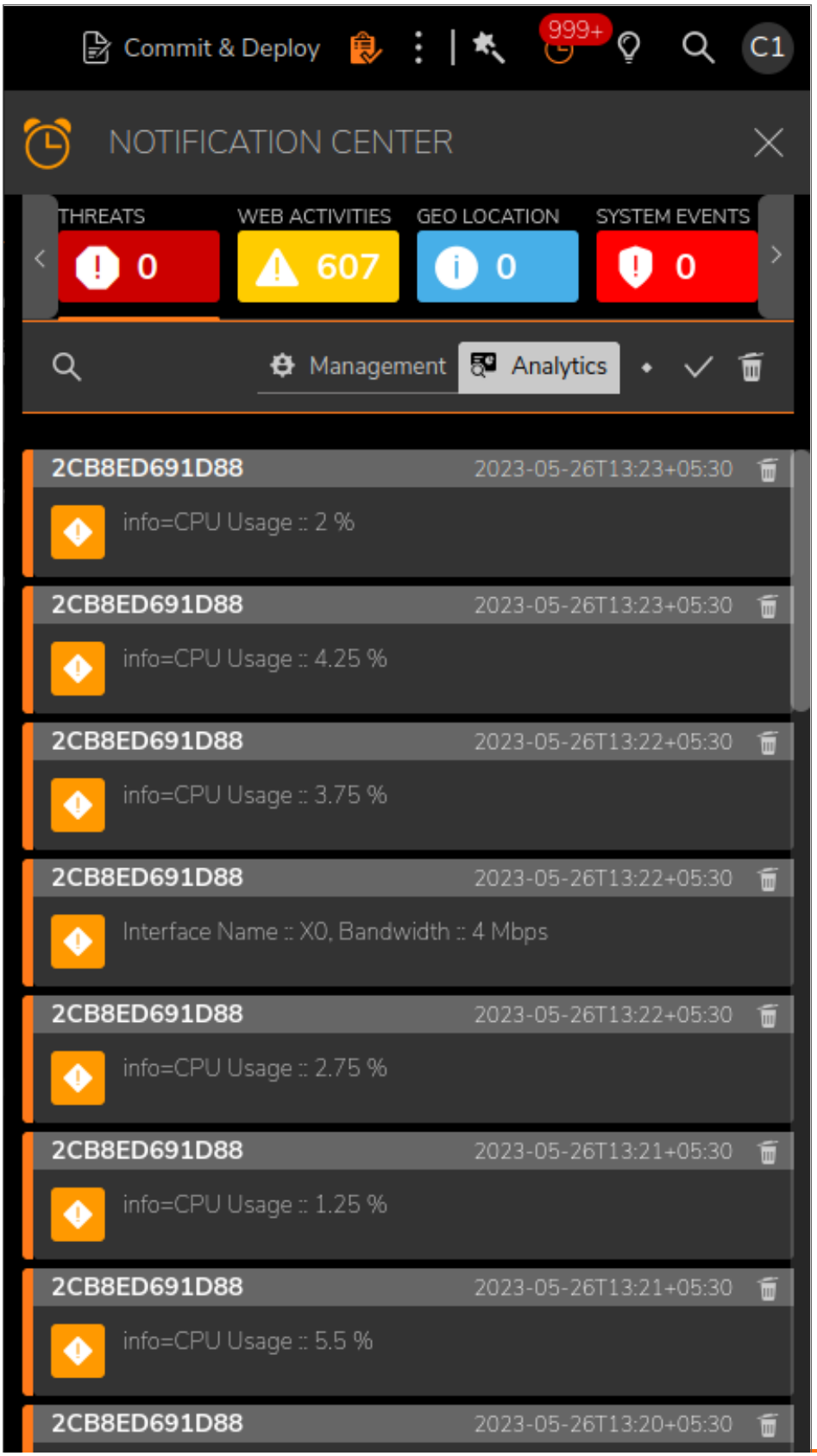
11

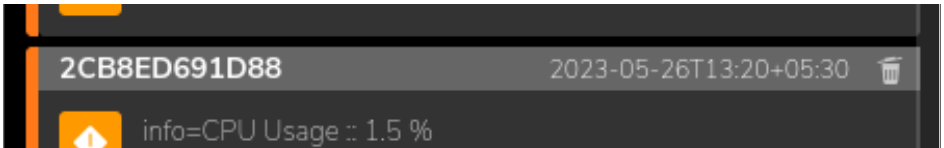
Notification Center

The Notifications Center shows administrators and users the status of their network infrastructure. It summarizes the number of notices, threats, operational notices, and general notices.

The Notification Center is a separate pane that provides the status and activities being monitored and recorded by NSM. After clicking on the Notifications Center icon at the top of the interface, the Notifications Center opens to show All alerts, Threats, Operations alerts, and General alerts. Each option shows how many unread alerts appear in that particular category.


Commit & Deploy
999+
C1
NOTIFICATION CENTER
ALL
4K
NETWORK USAGE
3K
THREATS
0
WEB ACTIVITIES
608
Management
Analytics
2CB8ED691D88
2023-05-26T13:24+05:30
info=CPU Usage :: 2 %
2CB8ED691D88
2023-05-26T13:24+05:30
Interface Name :: X0, Bandwidth :: 2 Mbps Interface Name :: X0, Connection Rate :: 5 Cps
2CB8ED691D88
2023-05-26T13:23+05:30
info=CPU Usage :: 2 %
2CB8ED691D88
2023-05-26T13:23+05:30
info=CPU Usage :: 4.25 %
2CB8ED691D88
2023-05-26T13:22+05:30
info=CPU Usage :: 3.75 %
2CB8ED691D88
2023-05-26T13:22+05:30
Interface Name :: X0, Bandwidth :: 4 Mbps
2CB8ED691D88
2023-05-26T13:22+05:30
info=CPU Usage :: 2.75 %
2CB8ED691D88
2023-05-26T13:21+05:30
2CB8ED691D88
2023-05-26T13:21+05:30
info=CPU Usage :: 5.5 %


Commit & Deploy
999+
C1
NOTIFICATION CENTER
THREATS
0
WEB ACTIVITIES
607
GEO LOCATION
0
SYSTEM EVENTS
0
Management
Analytics
2CB8ED691D88
2023-05-26T13:23+05:30
info=CPU Usage :: 2 %
2CB8ED691D88
2023-05-26T13:23+05:30
info=CPU Usage :: 4.25 %
2CB8ED691D88
2023-05-26T13:22+05:30
info=CPU Usage :: 3.75 %
2CB8ED691D88
2023-05-26T13:22+05:30
Interface Name :: X0, Bandwidth :: 4 Mbps
2CB8ED691D88
2023-05-26T13:22+05:30
info=CPU Usage :: 2.75 %
2CB8ED691D88
2023-05-26T13:21+05:30
info=CPU Usage :: 1.25 %
2CB8ED691D88
2023-05-26T13:21+05:30
info=CPU Usage :: 5.5 %
2CB8ED691D88
2023-05-26T13:20+05:30


2CB8ED691D88
2023-05-26T13:20+05:30
info=CPU Usage :: 1.5 %

In the search bar, you can search by firewall name, alert name, message or details.

To mark a single alert as read, click on the alert to acknowledge it. Click the white check-mark on top to mark all alerts in that view as read.

To delete a single alert, click on the trash icon on each alert. Click the trash icon at the top-right to delete all the alerts in that view.

12

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

Network Security Manager Reporting and Analytics Administration Guide
Updated - October 2024
232-005313-01 Rev P

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035